Allied Telesis™

AlliedView Network Management System

Administration Guide

Release 15.1

613-001999 Rev. B

Allied Telesis, Inc. reserves the right to make changes in specifications and other information contained in this document without prior written notice. The information provided herein is subject to change without notice. In no event shall Allied Telesis, Inc. be liable for any incidental, special, indirect, or consequential damages whatsoever, including but not limited to lost profits, arising out of or related to this manual or the information contained herein, even if Allied Telesis, Inc. has been advised of, known, or should have known, the possibility of such damages.

Table of Contents

14 Port Management - iMAP Devices - - - 396

15 Port Management - non-iMAP Devices - - - 496

1. The AlliedView Network Management System (NMS)

The AlliedView Network Management System (NMS) is a comprehensive tool to administer, operate and provision networks. The NMS collects and displays performance metrics, both real-time and historical. Faults are identified and logged, with alarm notification forwarded according to requirements. You can configure network elements remotely and maintain security by controlling user IDs and resource access.

The NMS displays information about the network in two ways:

- A graphical map interface displays the network and its managed objects both physically and functionally. You can start at the network level and drill down to the appropriate device.
- A set of forms lists the objects and their attributes.

1.1 The NMS Editions

There are two editions of the NMS: The Service Provider Edition (SE) and the Enterprise Edition (EE). The EE is a subset of the SE and does not include the complete feature set. The EE is intended for an enterprise customer managing a small network with a limited number of devices and does not include customer provisioning for voice, video, and data services.

1.2 Documentation Set

The following documents are available for the NMS:

- *AlliedView NMS Installation Guide*
- *AlliedView NMS Administration Guide*

You should also refer to the appropriate product guides for your network, including the following:

- *Software Reference for iMAP Series Switches*
- *Software Reference for SwitchBlade x3100 Series*
- *Allied Telesis Gateway Product Family Software Reference*

1.3 Contacting Allied Telesis

If you need assistance with this product, you may contact Allied Telesis technical support by going to the Support & Services section of the Allied Telesis web site at www.alliedtelesis.com/support. You can find links for the following services on this page:

- 24/7 Online Support - Enter our interactive support center to search for answers to your questions in our knowledge database, check support tickets, learn about Return Merchandise Authorization (RMA), and contact Allied Telesis technical experts.
- USA and EMEA phone support - Select the phone number that best fits your location and customer type.
- Hardware warranty information - Learn about Allied Telesis warranties and register your product online.
- Replacement Services - Submit an RMA request via our interactive support center.
- Documentation - View the most recent installation guides, user guides, software release notes, white papers and data sheets for your product.

- Software Updates - Download the latest software releases for your product.

For sales or corporate information, go to www.alliedtelesis.com/purchase and select your region.

2. Managed Devices

The NMS discovers and manages devices in a network. The NMS provides different levels of support for devices and not all devices are able to utilize all functions available in the NMS.

2.1 Devices Supported by the NMS

Devices are organized into the following categories:

- iMAP and AlliedWareNSP Devices
- iMGs
- AlliedWare Layer 3 Switches
- AlliedWare Plus Layer 3 Switches
- Layer 2 Switches
- AlliedWare Routers
- Metro Ethernet Products
- Wireless Access Products
- Third-Party Products

2.1.1 iMAP and AlliedWareNSP Devices

iMAP and AlliedWareNSP software releases are supported up to two releases prior to the current release.

Note: Release 17.0.x support begins with version 17.0.1. Release 17.0.0 is not supported.

TABLE 2-1 **iMAP and AlliedWareNSP Devices Supported by the NMS**

Family	Devices	Latest Software Release	Notes
iMAP 9000	9400 9101 9400-56 9700-56	17.0.x 17.2	
iMAP 9000	9700 9100 9102 9103	17.0.x 17.2	These devices are supported in previous versions of the NMS. They have not been tested with the current release.
iMAP 9000	9810	17.0.x 6.18.0.1	
SwitchBlade	SBx3112 SBx3106	17.0.x 6.18.0.1	

2.1.2 iMGs

TABLE 2-2 iMG Devices Supported by the NMS

Device	Latest Software Release	Notes
eDM1405	4.3.3	
iMG1405	4.3.3	This model can also contain an RF module backplate.
iMG1405W	4.3.3	
iMG1425	4.3.3	This model can also contain an RF module backplate.
iMG1425W	4.3.3	
iMG1505	4.3.3	
iMG1525	4.3.3	This model can also contain an RF module backplate.
iMG2426F	4.3.3	
iMG2504	4.3.3	
iMG2522	4.3.3	
iMG2524	4.3.3	
iMG2524F	4.3.3	Supports 100M/1000 on the WAN interface.
iMG2524H	4.3.3	Includes HPNA port.
iBG915FX	3-8-05	
iMG606BD	3-8-05	
iMG606BD-R2	3-8-05	
iMG606LH	3-7	This device is supported in previous versions of the NMS. It has not been tested with the current release.
iMG606SH	3-7	This device is supported in previous versions of the NMS. It has not been tested with the current release.
iMG613RF	3.8.3-14	Use RG613 in the Boot Configurator tool.
iMG616BD	3-8-05	
iMG616BD-R2	3-8-05	
iMG616LH	3-8-04	This device is supported in previous versions of the NMS. It has not been tested with the current release.
iMG616RF	3-8-04	This device is supported in previous versions of the NMS. It has not been tested with the current release.
iMG616RF+	3-8-04	This device is supported in previous versions of the NMS. It has not been tested with the current release.
iMG616SH	3-8-04	This device is supported in previous versions of the NMS. It has not been tested with the current release.

TABLE 2-2 iMG Devices Supported by the NMS (Continued)

Device	Latest Software Release	Notes
iMG616SRF+	3-8-04	This device is supported in previous versions of the NMS. It has not been tested with the current release.
iMG616W	3-8-05	
iMG624A	3-8-05	
iMG624A-R2	3-8-04	This device is supported in previous versions of the NMS. It has not been tested with the current release.
iMG624B	3-7	This device is supported in previous versions of the NMS. It has not been tested with the current release.
iMG626MOD	3-8-05	
iMG634A	3-8-05	
iMG634A-R2	3-8-05	
iMG634B	3-7	This device is supported in previous versions of the NMS. It has not been tested with the current release.
iMG634B-R2	3-8-05	
iMG634WA	3.7.4-30	
iMG634WA-R2	3-8-05	
iMG634WB	3-7	This device is supported in previous versions of the NMS. It has not been tested with the current release.
iMG634WB-R2	3-8-04	This device is supported in previous versions of the NMS. It has not been tested with the current release.
iMG646BD	3-8-05	
iMG646BD	3-8-04	This device is supported in previous versions of the NMS. It has not been tested with the current release.
iMG646BD-ON	3-8-05	
iMG646LH	3-7	This device is supported in previous versions of the NMS. It has not been tested with the current release.
iMG646MOD	3-8-05	
iMG646PX-ON	3-8-05	
iMG646SH	3-7	This device is supported in previous versions of the NMS. It has not been tested with the current release.
iMG726BD	3-8-05	
iMG726BD-ON	3-8-05	
iMG726MOD	3-8-04	This device is supported in previous versions of the NMS. It has not been tested with the current release.

TABLE 2-2 iMG Devices Supported by the NMS (Continued)

Device	Latest Software Release	Notes
iMG746MOD	3-8-05	
RG203TX-SIP/H323		This device is supported in previous versions of the NMS. It has not been tested with the current release.
RG203TX v2-SIP/H323		This device is supported in previous versions of the NMS. It has not been tested with the current release.
RG613BD	3-8-04	This device is supported in previous versions of the NMS. It has not been tested with the current release.
RG613LH	3-8-05	
RG613SH	3-7	This device is supported in previous versions of the NMS. It has not been tested with the current release.
RG613TX	3-8-05	
RG613TX	3-7	This device is supported in previous versions of the NMS. It has not been tested with the current release.
RG624A	3.5.0-83	
RG634	3.5.0-83	
RG656-LH	3-7	This device is supported in previous versions of the NMS. It has not been tested with the current release.
RG656-SH	3-7	This device is supported in previous versions of the NMS. It has not been tested with the current release.
RG656-TX	3-7	This device is supported in previous versions of the NMS. It has not been tested with the current release.
RG656BD	3-8-05	
Comtrend NexusLink CT-5631	310.9.1	Basic provisioning only. This device is supported in previous versions of the NMS. It has not been tested with the current release.

2.1.3 AlliedWare Layer 3 Switches

TABLE 2-3 AlliedWare Layer 3 Switches Supported by the NMS

Family	Devices	Latest Software Release	Notes
AT-8600	AT-8624POE AT-8624T/2M AT-8624XL AT-8624PS AT-8624EL AT-8648T/2SP	2.9.1-20	
AT-8700	AT-8724XL AT-8724XLDC AT-8724XLDCNEBS AT-8748XL AT-8748XLDC AT-8748SL AT-8748SL V2	2.9.1-20	The following releases are not supported by the NMS: • 2.6.1-04+ • 2.6.2 • 2.6.3
AT-9600	AT-9606SX/SC AT-9606T		These devices are supported in previous versions of the NMS. They have not been tested with the current release.
AT-9700	AT-9724TS AT-9748TSXP	3.03	These devices are supported in previous versions of the NMS. They have not been tested with the current release.
AT-9800	AT9812T AT9812TDC AT9812TF AT9816GB AT9816GBDC AT9816GF	2.9.1-20	These devices are supported in previous versions of the NMS. They have not been tested with the current release.
AT-9900	AT-9924SP AT-9924T AT-9924T4SP	2.9.1-20	If an <AT-9900> is part of an EPSR Domain, then to support EPSR management from the NMS, the NMS must be set as an SNMPv2 trap host on the device.
AT-9900s	AT-9924Ts	3.2.1-03	If an <AT-9900s> is part of an EPSR Domain, then to support EPSR management from the NMS, the NMS must be set as an SNMPv2 trap host on the device. This device is supported in previous versions of the NMS. It has not been tested with the current release.

TABLE 2-3 AlliedWare Layer 3 Switches Supported by the NMS (Continued)

Family	Devices	Latest Software Release	Notes
x900	900-24XS 900-24XT	3.2.1-05	These devices are supported in previous versions of the NMS. They have not been tested with the current release.
x900 - 48	x900-48FE x900-48FS	2.9.2-13	

2.1.4 AlliedWare Plus Layer 3 Switches

TABLE 2-4 AlliedWare Plus Layer 3 Switches Supported by the NMS

Family	Devices	Latest Software Release	Notes
AT-x510	AT-x510-28GTX AT-x510-52GTX AT-x510-28GPX AT-x510-52GPX ATx510DP-52GTX	5.4.4-0.0	
x600	AT-x600-24Ts AT-x600-24TsXP AT-x600-24Ts-POE AT-x600-48Ts AT-x600-48TsXP AT-x600-24Ts-POE+	5.4.2-3.11	The AlliedWare Plus x600 Series does not allow the modification of the Enhanced Recovery Mode if the EPSR domain is currently enabled. If a user attempts to do this, an error message is displayed. If an x600 is part of an EPSR Domain, then to support EPSR management from the NMS, the NMS must be set as an SNMPv2 trap host on the device.
x610	AT-x610-24Ts AT-x610-24Ts-PoE+ AT-x610-24Ts/X AT-x610-24Ts/X-PoE+ AT-x610-48Ts AT-x610-48Ts-PoE+ AT-x610-48Ts/X AT-x610-48Ts/X-PoE+ AT-x610-24SPs/X	5.4.4-0.0	The AlliedWare Plus x610 Series does not allow the modification of the Enhanced Recovery Mode if the EPSR domain is currently enabled. If a user attempts to do this, an error message is displayed. If an x610 is part of an EPSR Domain, then to support EPSR management from the NMS, the NMS must be set as an SNMPv2 trap host on the device. The Stack-XG card can be swapped during operation (e.g. to replace a faulty card), but for stacking to be activated the unit must be rebooted. (Stacking will not start unless the card is already inserted and the unit is rebooted.)

TABLE 2-4 AlliedWare Plus Layer 3 Switches Supported by the NMS (Continued)

Family	Devices	Latest Software Release	Notes
x900	x900-12XT/S ATx900-24XS ATx900-24XT ATx900-24XT-N	5.4.4-0.0	The AlliedWare Plus x900 Series does not allow the modification of the Enhanced Recovery Mode if the EPSR domain is currently enabled. If a user attempts to do this, an error message is displayed. If an x900 is part of an EPSR Domain, then to support EPSR management from the NMS, the NMS must be set as an SNMPv2 trap host on the device.
SwitchBlade	AT-SBx908 AT-SBx8112 AT-SBx8106	5.4.4-0.0	The AlliedWare Plus SBx908 Series does not allow the modification of the Enhanced Recovery Mode if the EPSR domain is currently enabled. If you attempt to do this, an error message is displayed. If an SBx908 is part of an EPSR Domain, then to support EPSR management from the NMS, the NMS must be set as an SNMPv2 trap host on the device.
AT-IX5-28GPX	AT-IX5-28GPX	5.4.4-0.0	
AT-IE200	AT-IE200-6GT AT-IE200-6GP AT-IE200-6FT AT-IE200-6FP	5.4.3-x.x	

2.1.5 Layer 2 Switches

TABLE 2-5 Layer 2 Switches Supported by the NMS

Family	Devices	Latest Software Release	Notes
AT-8000S	AT-8000S/16 AT-8000S/24 AT-8000S24/POE AT-8000S/48 AT-8000S/48POE	3.0.0.x	
AT-8000GS	AT-8000GS/24 AT-8000GS24/POE AT-8000GS/48	2.0.0.x	

TABLE 2-5 Layer 2 Switches Supported by the NMS (Continued)

Family	Devices	Latest Software Release	Notes
AT-8100S (AlliedWare Plus)	AT-8100S/24C AT-8100S/24 AT-8100S/24POE AT-8100S/48 AT-8100S/48POE AT-8100L	2.2.5.x	
AT-8100L (AlliedWare Plus)	AT-8100L/8POE	2.2.5.x	
AT-8200	AT-8224XL AT-8224SL AT-8216XL AT-8216FXL/SC AT-8216FXL/SMSC		These devices are supported in previous versions of the NMS. They have not been tested with the current release.
AT-8900	AT-8948	2.9.1-20	If an AT-8900 is part of an EPSR Domain, then to support EPSR management from the NMS, the NMS must be set as an SNMPv2 trap host on the device. This device is supported in previous versions of the NMS. It has not been tested with the current release.
AT-9000	AT-9000/28 AT-9000/28SP AT-9000/52	2.1.8	Mode LED indicator is fixed in the ACT Mode. The NMS has no provision for Mode Selection. Provision/De-provision button under Port Management is disabled since Profile Management function is not supported.
AT-9100	AT-9108		This device is supported in previous versions of the NMS. It has not been tested with the current release.
AT-x200	AT-x200-GE-28T AT-x200-GE-52T	5.4.4-0.0	
AT-x210	AT-x210-9GT AT-x210-16GT AT-x210-24GT	5.4.4-0.0	
AT-GS900M Series	AT-GS908M AT-GS916M AT-GS924M		These devices are supported in previous versions of the NMS. They have not been tested with the current release.
AT-GS950	AT-GS950/48PS	1.0.0	Basic support only. The release number displays as 0.0.0-0.
AT-MC2700	AT-MC2700		This device is supported in previous versions of the NMS. It has not been tested with the current release.

2.1.6 AlliedWare Routers

TABLE 2-6 AlliedWare Routers Supported by the NMS

Family	Devices	Latest Software Release	Notes
AT-AR100	AT-AR160 AT-AR130		These devices are supported in previous versions of the NMS. They have not been tested with the current release.
AT-AR200	AT-AR250E	1.0.6	Use AT Loader for upgrade. For AT Loader, contact your Allied Telesis representative or go to http://www.alliedtelesis.com/support. This device is supported in previous versions of the NMS. It has not been tested with the current release.
AT-AR260	AT-AR260S AT-AR260S v2		These devices are supported in previous versions of the NMS. They have not been tested with the current release.
AT-AR300	AT-AR300 AT-AR300 v2 AT-AR300L AT-AR300L v2		Use AT Loader for upgrade. For AT Loader, contact your Allied Telesis representative or go to http://www.alliedtelesis.com/support. These devices are supported in previous versions of the NMS. They have not been tested with the current release.
AT-AR450	AT-AR450S		This device is supported in previous versions of the NMS. It has not been tested with the current release.
MC2700	CentreCOM-MC2700	1.2.x	This device is supported in previous versions of the NMS. It has not been tested with the current release.
CentreCOM AR Series	AR415S AR550S AR560S AR570S	2.9.2-13	LLDP configuration per port is not supported and will return a ‘Function not supported’ error.
CentreCOM 8000 Series	8324XL 8316XLR 8324XLR 8424TX 8424XL	2.7.9-x	LLDP configuration per port is not supported and will return a ‘Function not supported’ error.
CentreCOM 9400 Series	CentreCOM-9424T	4.x	
CentreCOM 9400 Series	CentreCOM-9424T-SP	2.x	
CentreCOM FS Series	CentreCOM-FS926M CentreCOM-FS917M CentreCOM-FS909M	1.6.9	These devices are supported in previous versions of the NMS. They have not been tested with the current release.

TABLE 2-6 AlliedWare Routers Supported by the NMS (Continued)

Family	Devices	Latest Software Release	Notes
CentreCOM FS Series	CentreCOM-FS926M-PS CentreCOM-FS917M-PS CentreCOM-FS909M-PS	1.6.9	These devices are supported in previous versions of the NMS. They have not been tested with the current release.
CentreCOM FS Series	CentreCOM-FS808M	1.0.3	This device is supported in previous versions of the NMS. It has not been tested with the current release.
CentreCOM GS Series	CentreCOM-GS924M CentreCOM-GS916M CentreCOM-GS908M	1.6.6	These devices are supported in previous versions of the NMS. They have not been tested with the current release.
CentreCOM GS Series	CentreCOM-GS924Mv2 CentreCOM-GS916Mv2	2.1.0	These devices are supported in previous versions of the NMS. They have not been tested with the current release.
CentreCOM GS Series	CentreCOM-GS908Mv2 CentreCOM GS908v2-4PS	2.4.1	These devices are supported in previous versions of the NMS. They have not been tested with the current release.
CentreCOM 9048XL	CentreCOM 9048XL	2.1.0	This device is supported in previous versions of the NMS. It has not been tested with the current release.

2.1.7 Metro Ethernet Products

TABLE 2-7 Metro Ethernet Products Supported by the NMS

Family	Devices	Latest Software Release	Notes
EDM	EDM-S	1.0.0	Basic support only. The release number displays as 0.0.0-0.
MEx	MEx-244X-SE	1.0.0	Basic support only. The release number displays as 0.0.0-0.

2.1.8 Wireless Access Products

TABLE 2-8 Wireless Access Products Supported by the NMS

Family	Devices	Latest Software Release	Notes
AT-TQ2000	AT-TQ2450	2.0.2	Basic support only. The release number displays as 0.0.0-0.
AT-TQ3000	AT-TQ3600	2.0.2	Basic support only. The release number displays as 0.0.0-0.

2.1.9 Third-Party Products

TABLE 2-9 Third-Party Products Supported by the NMS

Family	Devices	Latest Software Release	Notes
GenBand	GB-G6	8-1-11 10-4-10	Supported for provisioning of MGCP voice lines and configuration backup and restore. This device is supported in previous versions of the NMS. It has not been tested with the current release.
GenBand	GB-G2	1.3.4	Supported for provisioning of MGCP voice lines and configuration backup and restore. This device is supported in previous versions of the NMS. It has not been tested with the current release.
Extreme BD	Extreme BD 8810 Extreme BD 8806	12.0	These devices are supported in previous versions of the NMS. They have not been tested with the current release.
Extreme Summit X250e	X250e-24t X250e-24p X250e-24x X250e-48t X250e-48p X250e-24tDC X250e-24xDC X250e-48tDC	12.0	These devices are supported in previous versions of the NMS. They have not been tested with the current release.
Extreme Summit X450a	X450a-24t X450a-48t X450a-24tDC X450a-24xDC X450a-24x X450a-48tDC	12.0	These devices are supported in previous versions of the NMS. They have not been tested with the current release.
Juniper	SSG 550M	6.1.0r6.0	This device is supported in previous versions of the NMS. It has not been tested with the current release.
NetScreen	NS-208 NS-50 NS-5XT	5.4.0r6.0 5.4.0r10.0, 5.3.0r7.0	These devices are supported in previous versions of the NMS. They have not been tested with the current release.
A10 AX3200	A100-AX3200		This device is supported in previous versions of the NMS. It has not been tested with the current release.

2.2 End-of-Support

Some Allied Telesis devices have reached end-of-support. Allied Telesis no longer officially supports them and does not guarantee they will continue to function correctly with this release of the NMS.

Devices that have reached end-of-support are organized into the following categories:

- Non-CPE Devices at End-of-Support
- CPE Devices at End-of-Support

2.2.1 Non-CPE Devices at End-of-Support

TABLE 2-10 Non-CPE Devices at End-of-Support

Family	Devices	Latest Software Release
AT-AR410	AT-AR410 AT-AR410 v2	2.7.1-x
AT-AR415	AT-AR415S	2.9.2-xx
AT-AR440	AT-AR440S	2.9.2-xx
AT-AR442	AT-AR442S	2.9.2
AT-AR700	AT-AR720 AT-AR740 AT-AR740DC	2.6.x-x
	AT-AR725 AT-AR725DC AT-AR745 AT-AR745DC	2.9.1-x
	AT-AR750S	2.9.2-xx
	AT-AR770S	2.9.2-xx
AT-8000	AT-8012M AT-8012MQS AT-8016FMT AT-8016FSC AT-8016FST AT-8016XL AT-8024 AT-8024GB AT-8024M AT-8026FC AT-8026T AT-8088MT AT-8088SC	3.3.x
AT-8300	AT-8312 AT-8324	2.0.x

TABLE 2-10 Non-CPE Devices at End-of-Support (Continued)

Family	Devices	Latest Software Release
AT-8500	AT-8516FSC AT-8524M AT-8525 AT-8524POE AT-8550GB AT-8550SP	1.4.x
AT-8800	AT-8824 AT-8824DC AT-8848 AT-8848DC	2.9.1-20
RG213	RG213-H323 RG213-MGCP RG213-SIP	6.x
Rapier	Rapier24 Rapier48	2.3.1-x 2.7.0-x
Rapier “G”	RapierG6 RapierG6flx RapierG6fmt RapierG6fsx	2.7.3-09
Rapier “i”	Rapier24i Rapier24iDCNEBS Rapier48i Rapier 48W	2.9.1-20
SwitchBlade (AlliedWare)	SB4104AC SB4104DC SB4108AC SB4108DC	2.7.5-09
Telesis T1000	T1000	1.3.x 1.6.x
iMAP	7100 7101 7102 7103 7104 7105 7112 7115 7400 7700	6.1.12

TABLE 2-10 Non-CPE Devices at End-of-Support (Continued)

Family	Devices	Latest Software Release
DTM	NM1000	-
AT-9400	AT-9408LC-SP AT-9424T AT-9424T-GB AT-9424T-POE AT-9424TS AT-9424T-SP AT-9424TS-XP AT-9448T-SP AT-9448TS-XP	-
AT-8324XL	AT-8324XL	-
AT-8724SL		-
AT-8748XL	AT-8748XL	-
AT-AR550S	AT-AR550S	-

2.2.2 CPE Devices at End-of-Support

TABLE 2-11 CPE Devices at End-of-Support

Device	Latest Software Release
AT-iMG624B	3-7
AT-iMG634B	3-7
AT-iMG634WA	3-7
AT-iMG634WB	3-7
AT-iBG910A	3-7
AT-iBG910B	3-7
AT-RG613FX	3-7
AT-RG613LX	3-7
AT-RG613SH	3-7
AT-RG613TX	3-7
AT-RG656LH	3-7
AT-RG656SH	3-7
AT-iMG664A	3-5
AT-iMG664B	3-5
AT-iMG664WA	3-5
AT-iMG664WB	3-5
AT-RG624A	3-5
AT-RG624AV2	3-5
AT-RG624B	3-5
AT-RG624BV2	3-5

TABLE 2-11 CPE Devices at End-of-Support (Continued)

Device	Latest Software Release
AT-RG634A	3-5
AT-RG634AV2	3-5
AT-RG634B	3-5
AT-RG634BV2	3-5
AT-RG644A	3-5
AT-RG644B	3-5
AT-RG623BD	2-5
AT-RG623FX	2-5
AT-RG623LH	2-5
AT-RG623LX	2-5
AT-RG623SH	2-5
AT-RG623TX	2-5
AT-iMG646BD-ON	3-8-04
AT-iMG646PX-ON	3-8-04
AT-RG656	3-8-04
AT-iMG624A	3-8-04
AT-iMG634A	3-8-04
AT-iMG613RF	3-8-04
AT-RG613BD	3-8-04
AT-RG613BDv2	3-8-04
AT-RG613LH	3-8-04

2.3 Devices Supported by SwimView

TABLE 2-12 Devices Supported by SwimView

AT-SB4104-00	8216XL	AR130
AT-SB4108-76	8216FXL/SC	MBRK16-10
9606SX/SC	8216FXL/SMSC	MBRK16-80
9606T	8124XL	MBMC115B
9108	8124	LBMC115A
8624PS	8116	MBMC140B
8624EL	8016XL	LBMC140A
8550	8008	MC2700-10
8525	3734TX	MC2602
8518	3734TX-1F	MC2601
8312	3726XL	WD1008L
9424Ts/XP-E	3726	WD1004
9424T/SP	3716TR plus	WD1002
9408LC/SP	3716TR	WD1001
9006SX/SC	RG107TX/B	AT-1331-10/80

TABLE 2-12 Devices Supported by SwimView

9006T	FS816M	RG107TX
ARX640S	GS908M V2-4PS	VS812TX
AR260S V2	9048XL	VS503EX
AR260S	IA810M	AT-TQ2403
RH609	3600 series	AT-TQ2450
FH812u	FH612TX	AT-TS HUB Series
FH824u	FH612TXS	AR160

2.4 Supported Functionality

The NMS supports different levels of functionality for different devices. The devices are grouped into the following familes:

- Allied Telesis, AlliedWare, and AlliedWare Plus Products
- Rapier Products
- AR and AT
- CentreCOM Products
- Metro Ethernet Products
- Wireless Access Products
- Third Party Products

2.4.1 Allied Telesis, AlliedWare, and AlliedWare Plus Products

TABLE 2-13 Feature Support for Allied Telesis, AlliedWare and AlliedWare Plus Products

Feature	iMAP 9000	AT-9800	x900 and x908	x510 and IX5	x600	x610	SBx3100	SBx8100	x200 and x210	IE200
View Chassis	Y	Y	Y[1]	Y	Y	Y	Y	Y	Y	-
Device Log Management	Y	Y	Y	Y	Y	Y	Y	Y	Y	-
Backup/Restore	Y	Y	Y	Y	Y	Y	Y	Y	Y	-
Command Script Mgmt.	Y	Y	Y	Y	Y	Y	Y	Y	Y	-
Configuration File Mgmt	Y	Y	Y	Y	Y	Y	Y	Y	Y	-
Syslog Management	Y	Y	Y	Y	Y	Y	Y	Y	Y	-
SNMPv2 Configuration	Y	Y	Y	Y	Y	Y	Y	Y	Y	-
SNMPv3 Configuration	N	Y	Y	Y	Y	Y	N	Y	Y	-
Software Configuration	Y	Y	Y	Y	Y	Y	Y	Y	Y	-
VLAN Configuration	Y	Y	Y	Y	Y	Y	Y	Y	Y	-
Card Management	Y	N	N	N	N	N	Y	N	N	-
Port Management	Y	Y	Y	Y	Y	Y	Y	Y	Y	-
Alarms/Events	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Performance Monitoring	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Telnet to Device	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SSH	Y	Y	Y[2]	Y[2]	Y[2]	Y[2]	Y[3]	Y[2]	Y[2]	Y
Stacking	n/a	n/a	Y	Y	Y	Y	n/a	N	N	-

TABLE 2-13 Feature Support for Allied Telesis, AlliedWare and AlliedWare Plus Products (Continued)

Feature	iMAP 9000	AT-9800	x900 and x908	x510 and IX5	x600	x610	SBx3100	SBx8100	x200 and x210	IE200
Browse Device	n/a	Y	Y	Y	Y	Y	n/a	Y	Y	-
Custom Load	Y	Y	Y	Y	Y	Y	Y	Y	Y	-
Config File Comparison	N	Y	Y	Y	Y	Y	Y	Y	Y	-
Network Services									Y	-
- Link Operations	Y	Y	Y	Y	Y	Y	Y	Y	Y	-
- VLAN	Y	Y	Y	Y	Y	Y	Y	Y	Y	-
- Profile management	Y	Y	Y	Y	Y	Y	Y	Y	Y	-
- QoS	Y	Y	Y	Y	Y	Y	Y	Y	Y	-
- EPSR	Y	Y	Y	Y	Y	Y	Y	Y	Y	-
- ESPR+	Y	N	Y	Y	Y	Y	Y	Y	Y	-
- CES	Y	n/a	n/a	n/a	n/a	n/a	n/a	N	N	-
LLDP Configuration	Y	n/a	Y	Y	Y	Y	Y	Y	Y	-
LAG	Y	N	Y	Y	Y	Y	Y	Y	Y	-
VCS Monitoring	N	N	Y	Y	Y	Y	N	N	N	-
Rediscover Device	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

1. For x900 stacked and SBx908 stacked, the chassis view shows both ETH0 ports as green. Only one should be green (the stack member with the connected eth0 port).
2. For AlliedWare Plus devices, only SSH version 2 is supported.
3. SSH cannot be used for Triple-Play Provisioning.

2.4.2 Rapier Products

TABLE 2-14 Feature Support for Rapier Products

Feature	AT-8600	AT-8700	AT-8800	AT-8900	AT-9900	x900
View Chassis	Y	Y	Y	Y	Y	Y
Device Log Management	Y	Y	Y	Y	Y	Y
Backup/Restore	Y	Y	Y	Y	Y	Y
Command Script Mgmt.	Y	Y	Y	Y	Y	Y
Configuration File Mgmt	Y	Y	Y	Y	Y	Y
Syslog Management	Y	Y	Y	Y	Y	Y
SNMPv2 Configuration	Y	Y	Y	Y	Y	Y
SNMPv3 Configuration	Y	Y	Y	Y	Y	Y
Software Configuration	Y	Y	Y	Y	Y	Y
VLAN Configuration	Y	Y	Y	Y	Y	Y
Card Management	N	N	N	N	N	N
Port Management	Y	Y	Y	Y	Y	Y
Alarms/Events	Y	Y	Y	Y	Y	Y
Performance Monitoring	Y	Y	Y	Y	Y	Y

TABLE 2-14 Feature Support for Rapier Products (Continued)

Feature	AT-8600	AT-8700	AT-8800	AT-8900	AT-9900	x900
Telnet to Device	Y	Y	Y	Y	Y	Y
SSH	Y	Y	Y	Y	Y	Y
Stacking	n/a	n/a	n/a	n/a	n/a	n/a
Browse Device	Y	Y	Y	n/a	Y	Y
Custom Load	Y	Y	Y	Y	Y	Y
Config File Comparison	Y	Y	Y	Y	Y	Y
Network Services						
- Link Operations	Y	Y	Y	Y	Y	Y
- VLAN	Y	Y	Y	Y	Y	Y
- Profile management[1]	Y	Y	Y	Y	Y	Y
- QoS[1]	Y	Y	Y	Y	Y	Y
- EPSR	Y	Y	Y	Y	Y	Y
- ESPR+	N	N	N	N	N	N
- CES	n/a	n/a	n/a	n/a	n/a	n/a
LLDP Configuration	Y	Y	Y	Y	Y	Y
LAG	Y	N	N	N	N	N
VCS Monitoring	N	N	N	N	N	N

[1] Profile Management and QoS are supported in release 2.5.1 and above.

2.4.3 AR and AT

TABLE 2-15 Feature Support for AR and AT Products

Support Features	AR 700	AR 400	AR 400s	AT-8324	AT-8000	AT-8500	AT-9700	AT-8000S	AT-8000GS	AT-8100S and AT-8100L	AT-9000
View Chassis	Y			Y	Y	Y	Y	Y	Y	Y[1]	Y[2]
Provision											
- Backup	Y	Y	Y	N	N	N	N	Y	Y	Y	Y
- Restore	Y	Y	Y	N	N	N	N	N	N	Y	Y
- Command Script Mgmt.	Y	Y	Y	N	N	N	N	N	N	N	N
- Configuration File Mgmt	Y	Y	Y	N	N	N	N	Y	Y	N	Y
- Device Information	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
- Device Log Management	Y	Y	Y	N	N	N	N	N	N	Y	Y
- SNMP Agent	Y	Y	Y	N	N	Y	Y	Y	Y	Y	Y
- SNMPV2 Configuration	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

TABLE 2-15 Feature Support for AR and AT Products

Support Features	AR 700	AR 400	AR 400s	AT-8324	AT-8000	AT-8500	AT-9700	AT-8000S	AT-8000GS	AT-8100S and AT-8100L	AT-9000
- SNMPV3 Configuration	Y	Y	Y	N	N	Y	Y	Y	Y	Y	Y
- Software Configuration	Y	Y	Y	N	N	N	N	Y	Y	Y	Y
- Text File Comparison	Y	Y	Y	-	-	N	Y	Y	Y	N	Y
- Configure VLAN	-	Y	Y	Y	Y	N	N	N	N	Y	Y
- Card Management	-	-	-	-	-	-	-	N	N	N	Y
- Port Management	-	-	-	-	-	-	-	Y	Y	Y	N
- Syslog	Y	N	N	N	N	N	N	N	N	Y[3]	Y[3]
- SSH	Y	Y	Y	N	N	Y	Y	N	N	Y[4]	Y
Network Service											
- Link Operations	-	Y	Y	Y	Y	N	N	Y	Y	Y	Y
- VLAN	-	-	-	All	All	N	N	Y	Y	Y	All
- Profile Mgmt.	-	Y	Y	N	N	N	N	N	N	N	N
- QoS	-	Y	Y	N	N	N	N	N	N	N	N
- EPSR	-	-	-	N	N	N	-	-	-	N	N
- CES	-	-	-	-	-	N	-	-	-	-	-
LLDP Configuration	N	N	N	N	N	Y	N	Y	Y	Y	N
LAG	N	-	-	-	-	Y		Y	Y	N	N
VCS Monitoring	N	-	-	-	-	Y	-	Y	Y	Y	N
Alarms/Events	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Performance	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Browse Device	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Rediscover Device	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

[1] If the devices are in stacked configuration and a SFP module is inserted to the stack member 2; the CLI command 'show system pluggable' will not show SFP modules for stack members. If the device stack ID is not 0, Chassis View and Port Management shows all ports are down. This is due to doing the SNMP GET of the ifOperStatus <portinterface> returns the value '2', which means down. Finally, the incorrect LED turns green when an SFP module is inserted in the SFP port and its corresponding redundant RJ-45 port is active.

[2] Incorrect LED turns green when an SFP module is inserted in the SFP port and its corresponding redundant RJ-45 port is active.

[3] Supported, but unable to set device logs to disable. Syslog status cannot be disabled.

[4] Open SSH prompts for the password twice.

2.4.4 CentreCOM Products

TABLE 2-16 AlliedView NMS CentreCOM Product Support

Support Features	AR Series	8000 Series	MC2600	MC2700	9400 Series	GS Series	FS Series	9048XL
View Chassis	Y	Y	Y[1,2]	Y[3,4]	Y	Y	Y	Y
Provision								
- Backup/Restore	Y	Y	Y	Y	Y	Y	Y	Y
- Command Script Mgmt.	Y	N	-	-	-	N	N	N
- Configuration File Mgmt	Y	Y	Y	Y	Y	Y	Y	Y
- Device Information	Y	Y	Y	Y	Y	Y	Y	Y
- Device Log Management	Y	Y	Y	Y	Y	Y	Y	Y
- SNMP Agent	Y	Y	Y[5]	Y[5]	Y[6]	Y	Y	Y
- SNMPV2 Configuration	Y	Y	Y	Y	Y	Y	Y	Y
- SNMPV3 Configuration	Y	Y[7]	-	-	Y	-	N	-
- Software Configuration	Y	Y	Y	Y	Y[8]	Y	Y	Y
- Text File Comparison	Y	Y	Y	Y	Y	Y	Y	Y
- Configure VLAN	Y	Y	-	-	Y	Y	Y	Y
- Card, Port Management	Y[9]	Y[9]	-	-	Y[9]	N	N	N
- Syslog	Y	Y	Y[10]	Y[10]	Y[10]	Y	Y[10]	Y[10]
- SSH	Y	N[11]	-	-	Y	-	-	-
Network Services								
- Link Operations	Y	Y	-	-	Y	Y	Y	Y
- VLAN	Y	Y	-	-	Y	Y	Y	Y
- Profile Mgmt	N	N	-	-	N	N	N	N
- QoS	N	N	-	-	N	N	N	N
- EPSR	N	Y	-	-	Y[12]	Y	Y[13,14]	Y
- CES	N	Y	-	-	-	N	N	N
LLDP Configuration	Y[15]	Y[15,16]	-	-	-	N	N	N
Alarms/Events	Y	Y	Y	Y	Y[17]	Y	Y	Y
Performance	Y	Y	Y	Y	Y	Y	Y	Y
Browse Device	Y	N	Y	Y	-	Y	Y	Y
Rediscover Device	Y	Y	Y	Y	Y	Y	Y	Y

[1] There is no info via SNMP or CLI that shows the duplex mode. The duplex LED will always be gray.

[2] The color of disabled port will not turn orange when module/port is disabled via CLI

[3] There is no info via SNMP or CLI that shows the duplex mode. The duplex led will always be gray.

[4] The color of disabled port will not turn orange when module/port is disabled via CLI

[5] Can only have a maximum of two SNMP communities.

[6] Disregard the SNMP Version parameter when creating and modifying SNMP Community.

[7] 8748XL is not supported.

[8] NMS will return the Application Software Version name which was shown when commands ‘show switch’ and ‘show system’ was executed on the device instead of the exact filename of the loaded release file.

9. Support for Port Management and Card Management is not applicable.
10. Enable and Disable of Device Log(s) are the only supported operations; only the default syslog server and filter are available.
11. Only the 8748XL supports SSH.
12. “Create/Protect EPS Data Ring”, “View EPS Data Protection” and “Modify Protection Domain” are not supported.
13. FS808 devices do not support EPSR.
14. When creating EPSR, ports should not be part of STP.
15. LLDP configuration per port is not supported.
16. Only 8700 devices support LLDP configuration module.
17. There will be no event generated for 'authenticationFailure' trap when using SNMPv3. It is only applicable when using SNMPv1 or SNMPv2c.

2.4.5 Metro Ethernet Products

TABLE 2-17 Feature Support for Metro Ethernet Devices

Features	EDM	MEx
View Chassis	-	-
Provision	-	-
- Backup/Restore	N	N
- Command Script Mgmt.	-	-
- Configuration File Mgmt	-	-
- Device Information	-	-
- Device Log Management	-	-
- SNMP Agent	-	-
- SNMPV2 Configuration	N	N
- SNMPV3 Configuration	N	N
- Software Configuration	-	-
- Text File Comparison	-	-
- Configure VLAN	-	-
- Card, Port Management	-	-
- Syslog	-	-
- SSH	N	N
Network Services	-	-
- Link Operations	-	-
- VLAN	-	-
- Profile Mgmt	-	-
- QoS	-	-
- EPSR	-	-
- CES	-	-
LLDP Configuration	-	-
LAG	-	-
VCS Monitoring	-	-
Alarms/Events	Y	Y
Performance	Y	Y

TABLE 2-17 Feature Support for Metro Ethernet Devices

Features	EDM	MEx
Browse Device	Y	Y
Rediscover Device	Y	Y

2.4.6 Wireless Access Products

TABLE 2-18 Feature Support for Wireless Devices

Features	AT-TQ2000	AT-TQ3000
View Chassis	-	-
Provision	-	-
- Backup/Restore	-	-
- Command Script Mgmt.	-	-
- Configuration File Mgmt	-	-
- Device Information	-	-
- Device Log Management	-	-
- SNMP Agent	-	-
- SNMPV2 Configuration	-	-
- SNMPV3 Configuration	-	-
- Software Configuration	-	-
- Text File Comparison	-	-
- Configure VLAN	-	-
- Card, Port Management	-	-
- Syslog	-	-
- SSH	-	-
Network Services	-	-
- Link Operations	-	-
- VLAN	-	-
- Profile Mgmt	-	-
- QoS	-	-
- EPSR	-	-
- CES	-	-
LLDP Configuration	-	-
LAG	-	-
VCS Monitoring	-	-
Alarms/Events	Y	Y
Performance	-	-
Browse Device	Y	Y
Rediscover Device	Y	Y

2.4.7 Third Party Products

Third party devices have limited support in the NMS. The NMS can discover and display them in the topology map but you must configure them outside the NMS.

TABLE 2-19 Feature Support for Third Party Devices

Features	Juniper	Extreme Summit	Extreme BD	NetScreen	G6/ G2
View Chassis	-	-	-	-	N
Provision	-	-	-	-	
- Backup/Restore	Y	Y Can specify additional files for backup	Y Can specify additional files for backup	-	Y
- Command Script Mgmt.	-	-	-	-	Y
- Configuration File Mgmt	-	-	-	-	N
- Device Information	-	-	-	-	N
- Device Log Management	-	-	-	-	Y
- SNMP Agent	-	-	-	-	N
- SNMPV2 Configuration	Y	Y	Y	N	N
- SNMPV3 Configuration	Y	Y	Y	N	N
- Software Configuration	-	-	-	-	N
- Text File Comparison	-	-	-	-	N
- Configure VLAN	-	-	-	-	N
- Card, Port Management	-	-	-	-	N
- Syslog	-	-	-	-	N
- SSH	N	Y	Y	Y	N
Network Services	-	-	-	-	N
- Link Operations	-	-	-	-	-
- VLAN	-	-	-	-	
- Profile Mgmt	-	-	-	-	N
- QoS	-	-	-	-	N
- EPSR	-	-	-	-	N
- CES	-	-	-	-	N
LLDP Configuration	-	-	-	-	N
LAG	-	-	-	-	N
VCS Monitoring	-	-	-	-	N
Alarms/Events	-	-	-	-	N
Performance	-	-	-	-	N
Browse Device	-	-	-	-	N
Rediscover Device	-	-	-	-	N

3. Starting Up

The AlliedView Network Management System (NMS) offers a variety of startup methods, with each having its advantages:

- Application Client - This is used entirely on the AlliedView NMS server.
- Application Start (Web Start) - This is the **preferred method** when accessing the NMS from a remote location. It requires Web Start (JRE: 1.6.0_nn) on the client. (This is also the first option on the Logon screen using a browser.) Refer to Figure 3-2.
- Web Client (HTML) - All that is required is a browser that meets the criteria listed in Table 3-1. (This is the second option on the Logon screen.)
- Applet Client - This involves loading of the correct applet and can be local or remote to the server. It requires the Java Runtime Environment (JRE)1.6.0_nn. (This is a link at the bottom of the Logon screen.)

Note: The monitor used by the NMS client should have a resolution of 1280x1024 or better.

Table 3-1 lists the client types and the startup methods for each platform.

TABLE 3-1 User Interfaces and Startup Methods for the NMS

Client Type	Description	Windows	Linux
Web Start	You must have the correct browser to view the logon screen. These are the same as for the Web Client (HTML) option. This is used for terminals connected remotely to the NMS server. It is the **preferred** method of accessing the NMS from a remote location, since the correct applet is automatically included as part of the startup and does not require reloading on subsequent client startups	On the Logon screen, select the **Launch** button for the **Application Client (Web Start)**. Refer to "Using the Browser" on page 40.	The same as Windows

TABLE 3-1 User Interfaces and Startup Methods for the NMS (Continued)

Client Type	Description	Windows	Linux
Web Client (HTML)	This uses a browser using HTML only and can be used from remote and local interfaces. Browsers: - Internet Explorer 7 and 8 - Firefox 3.0 or above	On the Logon screen, select the second option, and input the user Name and Password Refer to "Using the Browser" on page 40.	The same as Windows
Application	This is used for terminals connected directly to the NMS server and includes all software needed.	From the *Start* menu of windows, select *Programs->Allied Telesis -> AlliedView NMS ->Start NMS Client.* Directly from the home directory of the NMS Client, go to the **bin** directory and invoke the **startApplicationClient.bat** file.	From the home directory of the NMS client, go to the **bin** directory and invoke the **startApplicationClient.sh** file.

Note: When using the html client type, the browser property should be set so that for every visit to the page there is a check for the newer versions of the stored page. This is to ensure that any changes made are immediately reflected in the GUI. Refer to "Setting Web Browser Caching" on page 1129 for an example.

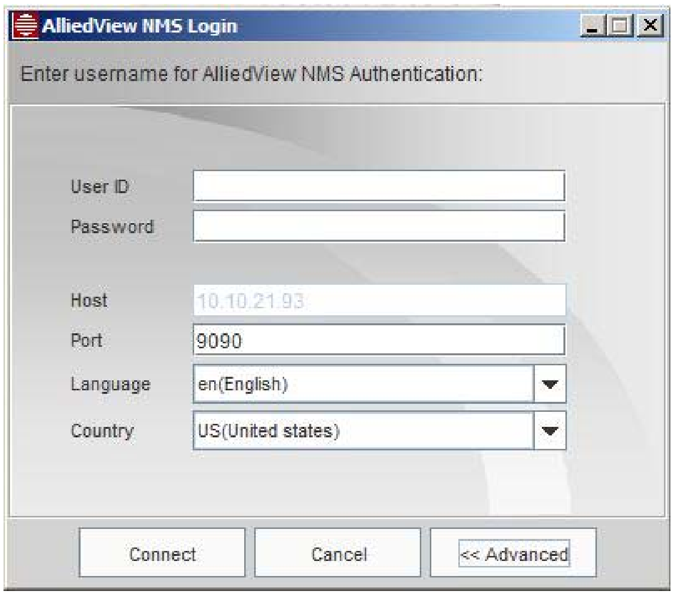
3.1 Logging In

3.1.1 Using the Client

By choosing the *Start NMS Client* option from the *Start* menu, you get the **AlliedView NMS Authentication** dialog box. By default, the username and password are **root** and **public**, respectively. You can also change the username and password based on your requirements.

By default the form shows only the User ID and Password. If you select the Advanced button you see the figure below. Included is the name of the host machine on which the NMS server is running, which is usually already filled in. The default port number is 9090. If the **Show Console** option is checked, the **Logs** console will appear on the screen; otherwise it will not be shown.

Enter the username and password, then click **Connect** to connect to the host server.



AlliedView NMS Login

Enter username for AlliedView NMS Authentication:

User ID

Password

Host 10.10.21.93

Port 9090

Language en(English)

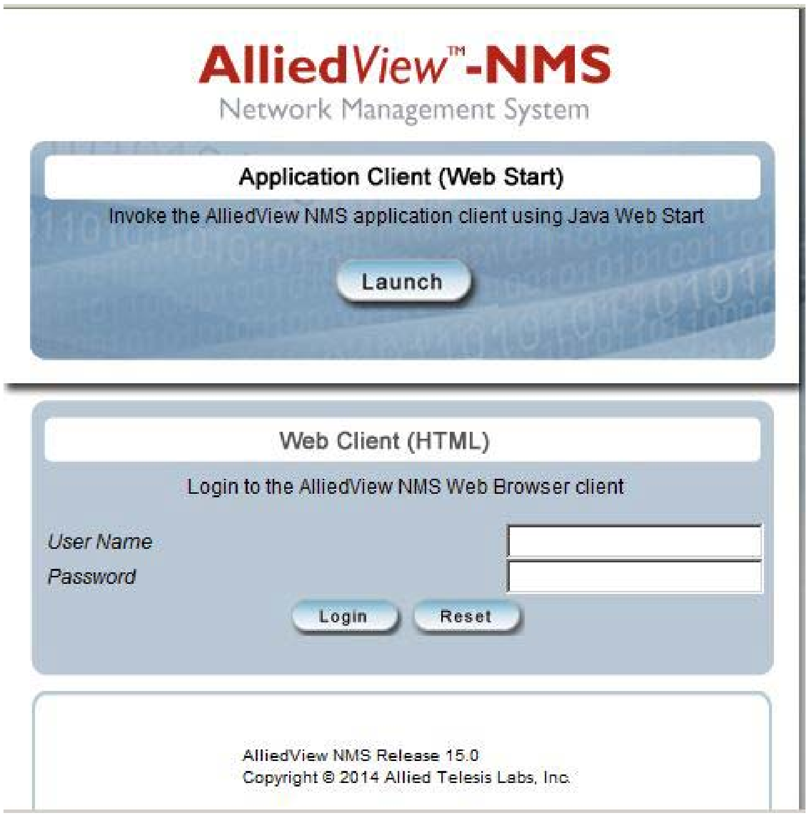
Country US(United states)

FIGURE 3-1 Logon Using the Application Client (Advanced Button)

3.1.2 Using the Browser

Connect the host from the browser after providing the name of the host and the port number as the Uniform Resource Locator (URL), such as **http://<hostname>:9090.** The logon screen (Figure 3-2) appears. Choose one of the three logon methods.

Note: *The login and password entry field on the main AlliedView NMS web page are not used when the user selects "Application Client (Web Start)". The Web Start Client log in procedure will prompt for the user/password on another window displayed later in the start up process.*



AlliedView™-NMS

Network Management System

Application Client (Web Start)

Invoke the AlliedView NMS application client using Java Web Start

Web Client (HTML)

Login to the AlliedView NMS Web Browser client

User Name

Password

AlliedView NMS Release 15.0
Copyright © 2014 Allied Telesis Labs, Inc.

FIGURE 3-2 Logon Screen Using the Browser

3.2 Connecting to the NMS Server

3.2.1 First Time Connection (Configuring the Password)

The NMS provides the option to configure your password once you have logged into the application client or the browser client for the first time. The **Password Configuration** dialog box appears by choosing the *Tools -> Change Password* menu item. Refer to the following figure. You can type in your new password and set the time duration for which this password is to remain valid. Refer to the following figure.

Note: The expiration duration is the number of days before the password expires; 0 (or negative number) means no expiration. To force a password to expire, the user must set the duration for one day, and the password will expire on the second day.

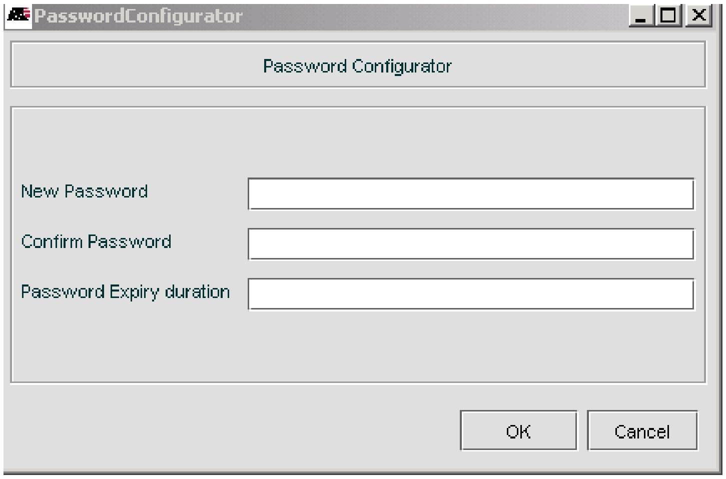


FIGURE 3-3 Setting a New Password

3.2.2 Possible Connection Failures

3.2.2.1 Password Has Expired

If you try to log in to the NMS Server after your password has expired, you will get an error message. You can reset the password.

3.2.2.2 User Account Has Expired

If your account has expired, a **Login Failed** dialog box pops up. In this condition, you will be unable to access the Java Client until your user account is re-activated by the NMS Administrator through the Security Administration User Interface (UI).

3.2.2.3 User is Disabled

If your user account is disabled by the NMS Administrator through the Security Administration UI, you will be unable to access the Java Client until your account is re-enabled. A **Login Failed** dialog box will pop up indicating that your account is disabled.

3.2.2.4 Maximum Number of Client Sessions is Reached

If you try to log in to the NMS Server while five other users are already logged in, your login attempt will fail with an error message indicating that the maximum number of sessions has been exceeded. The AlliedView NMS Server supports a maximum of five simultaneous client sessions. If you receive this error message, you will have to wait until one or more of the current users log out before you can log in.

3.2.2.5 Client-Server Connection is Lost

If you lose your connection with the NMS server, a dialog box with a message pops up. Restart the client using the methods in Table 3-1.

3.3 The Application Screen

When you log in to the application interface, the initial screen that is displayed shows the map symbols representing the discovered network devices. An example is shown in Figure 3-4. Callouts in the figure identify the various screen areas.

Note: For display purposes, the entire map is not shown in the figure.

You can find the Panel-Specific Menu Bar, Toolbar, Map Toolbar, NMS Tree, Alarm Count Panel, Status Bar, and the NMS Display Panel displayed in the user interface.

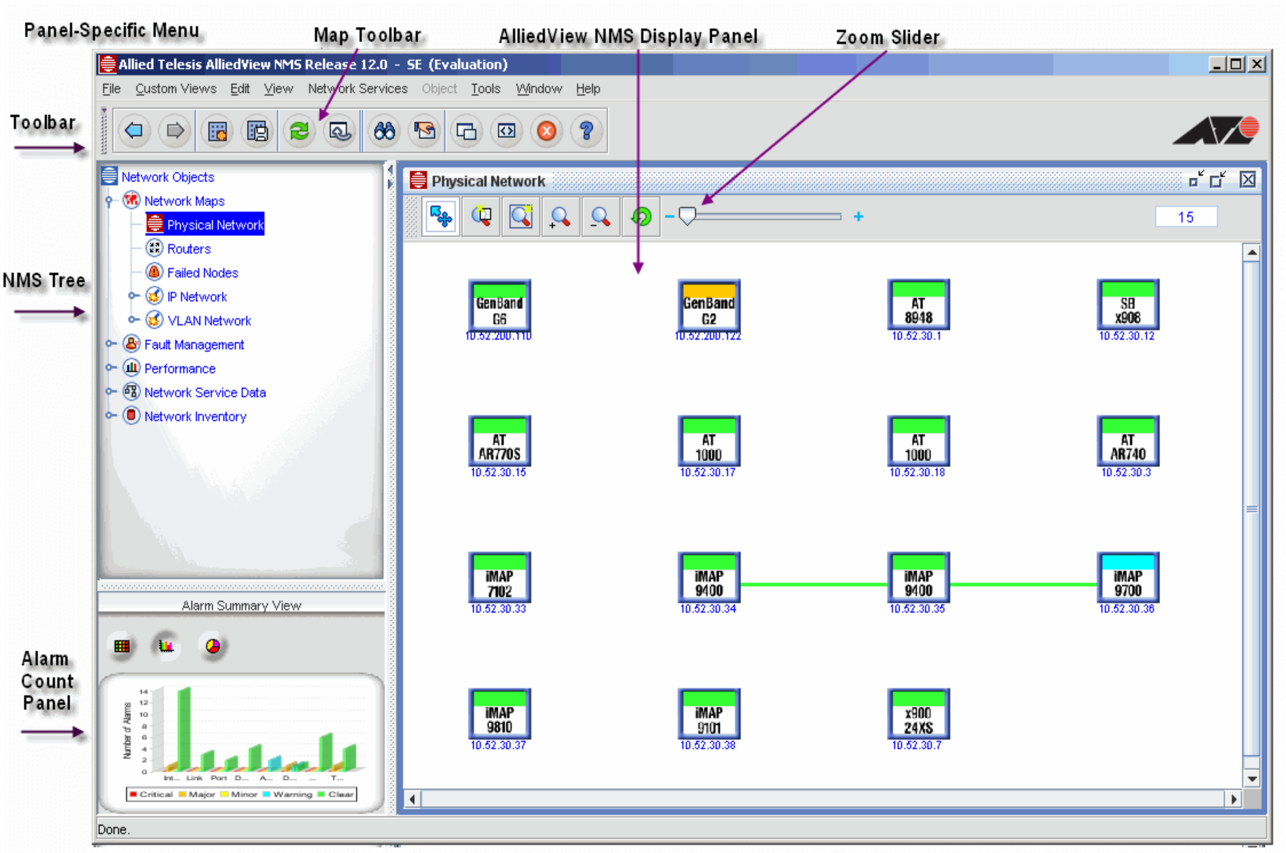


FIGURE 3-4 Layout of Initial Screen for Application Client

3.3.1 Panel-Specific Menu Bar

The Panel-Specific Menu Bar is positioned at the top edge of the display area. This menu bar contains the labels of drop-down menus attached to it. Right-clicking a menu label displays the drop-down list of menu items for that menu label. In a drop-down menu, separator lines distinguish types of tasks. The menu list is context-specific and will vary depending on which node in the NMS Tree is being displayed in the NMS Display Panel. However, a few of the items are common to all of the displays. These include:

- *File* - Provides control of the NMS client tool and the displays. The items include:
  - *Back* - Moves the display in the NMS Display Panel back to the previous display
  - *Forward* - Moves the display in the NMS Display Panel forward to the next display
  - *Detach* - Puts the current display in the NMS Display Panel in a separate window
  - *Close* - Closes the current display in the NMS Display Panel
  - *Close All* - Closes all open displays in the NMS Display Panel
  - *Broadcast Message* - Sends a message to other NMS users
  - *Exit* - Exits the NMS Client
- *Tools* - Provides various tools related to the NMS. The items include:
  - *View Tasks* - Displays a list of currently scheduled tasks

  - *Manage CLI Users* - Provides Command Line Interpreter (CLI) user management functions
  - *System Log Configuration* - Provides configuration functions for System Log Management
  - *NMS Database Backup* - Provides NMS database backup functions
  - *Discovery Configurator* - Provides configuration functions for NMS discovery
  - *Security Administration* - Provides security administration functions
  - *Change Password* - Allows you to change your password
  - *Application Manager* - Provides application management functions
  - *Mib Browser* - Provides Management Information Base (MIB) browsing functions
  - *Open Telnet* - Allows you to telnet to another device
- *Window* - Provides control for the NMS client display windows. The items include:
  - A radio-button list of the most recently accessed panels
  - *Cascade* - Cascades the open windows in the NMS Display Panel
  - *Tile Horizontal* - Tiles the open windows horizontally in the NMS Display Panel
  - *Tile Vertical* - Tiles the open windows vertically in the NMS Display Panel
  - *Save Location and Size* - Saves the current size and screen location of the NMS display
  - *Show Toolbar* - Displays or hides the Toolbar
- *Help* - Provides Help information for the AlliedView NMS.

The context-specific menu items will be described later in this document.

3.3.2 Toolbar

The Toolbar displays a collection of actions, commands, or control functions. Toolbars are used to display frequently used components. It is placed below the menu bar and has various tools for different nodes. A tool tip is provided for each tool. The Toolbar is movable and floatable. The tools that appear on the Toolbar will vary depending on which NMS Tree node is being displayed in the NMS Display Panel. The Toolbar for the Network Maps node is shown in the following figure.

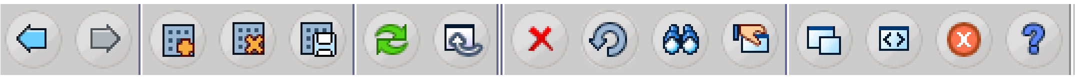


FIGURE 3-5 Example Toolbar

The Toolbar icons and their function are listed in the following table.

TABLE 3-2 Toolbar Tools and their Function

Toolbar Icon	Function
⇦	Move backward to the previous display in the NMS Display Panel.
⇨	Move forward to the next display in the NMS Display Panel.
▦	Add a new map.
☒	Delete the currently displayed map.

TABLE 3-2 Toolbar Tools and their Function

Toolbar Icon	Function
💾	Save the currently displayed map.
🔄	Refresh the map data.
⟲	Re-layout the currently displayed map.
✕	Delete the currently selected item(s) in the map.
↺	Undo the last Add or Delete.
🔍	Search a map or display for a specific string.
✎	Access the properties for the selected item or the currently displayed map. If no object is selected in the map, the map properties are displayed. If multiple objects are selected, a property sheet for each selected item will be displayed.
⧉	Detach the current display in the NMS Display Panel from the NMS Display Panel. The display will appear in a separate window from the main NMS window.
<>	Launch the NMS HTML user interface.
⊗	Stop the currently in-progress action.
?	Access the AlliedView NMS Help information.
+	Add a custom view.
✎	Modify a custom view.
✕	Remove a custom view.

Note: *Not all of the icons listed in Table 3-2 are shown in Figure 3-5. The actual icons that appear will depend on which tree node is being displayed in the NMS Display Panel.*

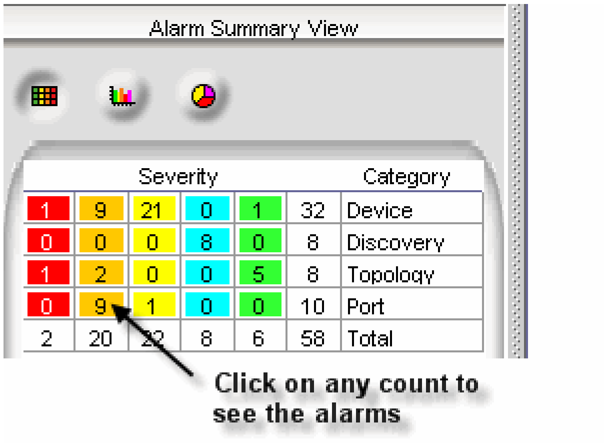
3.3.3 NMS Tree

The NMS Tree is built by the user to display a set of hierarchical data. The fundamental object in a tree is called a *node*, which represents a data item in the given hierarchical set. Thus, a tree is composed of one or more nodes. The root node is the top node of the hierarchical data.

Nodes inside the root nodes are called *child nodes*. Nodes that contain no child nodes are called *leaf nodes*. By choosing a particular node, the corresponding panel will be displayed on the right-side frame.

3.3.4 Alarm Count Panel

The Alarm Count panel shows the count of alarms of each severity (major, minor, critical, etc.) for each category. The Alarm Count panel is located below the tree. An example is shown in the figure.



Severity						Category
1	9	21	0	1	32	Device
0	0	0	8	0	8	Discovery
1	2	0	0	5	8	Topology
0	9	1	0	0	10	Port
2	20	22	8	6	58	Total

Click on any count to see the alarms

FIGURE 3-6 Example Alarm Count Panel

The colors used in the alarm display and their meaning are shown in the following table.

TABLE 3-3 **Status Colors and their Meaning**

Description	Sample	Meaning
Red	🟥	Critical alarm condition
Orange	🟧	Major alarm condition
Yellow	🟨	Minor alarm condition
Light Blue	🟦	Warning
Green	🟩	No alarm-normal operation
Gray	▨	Not managed by the NMS

The categories are as follows:

- Topology - Alarms in the Topology map
- Fan - Fan Failures
- Provisioning - Components have not been provisioned properly
- Rediscovery - Alarms for rediscovery (mainly for iMG./RG)
- Interface -
- Discovery - Alarms from the discovery process
- VLAN Interface -
- Device - Alarms received from devices
- Port - Alarms relevant for device ports

Clicking an alarm count displayed in the Alarm Count panel displays the alarms of the specific severity in the corresponding Alarm panel. This panel is updated automatically and the counts can be seen all the time, regardless of the current View. The tool tip and the cursor shape change when the mouse pointer is pointed on alarm counts. By clicking the counts in the alarm count panel, you can find the display of the respective alarms on the Alarms display in the NMS Display Panel.

Note: The Alarms display panel is described later in this document.

3.3.5 Status Bar

The Status Bar indicates the status of the process going on such as **Done** or if all the contents are loaded or **loading**... if the process is in progress. The transformation of the status bar color from dark blue to green takes place during the loading of the product.

3.3.6 AlliedView NMS Display Panel

The NMS Display Panel is the main window and shows the results of what is selected in the tree or in a menu.

Note: As you click on different nodes or menu items, the displays will stack on top of each other. Use the Window menu options as described in "Controlling Windows" on page 47 to control how the displays are stacked.

3.3.7 MAP Toolbar

The Map Toolbar displays a collection of commonly performed actions, commands, or control functions specific to the map being displayed. The Map Toolbar is described in "Using the Map Toolbar" on page 54.

3.3.8 Zoom Slider

The zoom slider allows you to quickly zoom in or zoom out the map display. It appears only on Network Maps. Left-clicking the slider button while dragging it to the right zooms in, while dragging it to the left zooms out.

3.3.9 Controlling Windows

The pull-down *Windows* menu allows the user to control how the display panels are organized.

- The current open displays are listed as a radio button list with the display currently in the foreground checked. Clicking one of the display buttons brings the corresponding display to the foreground.
- *Cascade*, *Tile Horizontal*, and *Tile Vertical* control the layout of the displays.
- *Save Location and Size* freezes the current window size. Selecting again toggles back.
- *Show Toolbar* checkbox toggles showing of the Toolbar. When checked, the Toolbar is displayed.

3.3.10 Allied Telesis Name

Clicking on the Allied Telesis name brings up the Allied Telesis Networks web site.

3.4 Password Configuration

The NMS provides the option to configure your password once you have logged into the application client or the browser client for the first time. The **Password Configuration** dialog box appears by choosing the *Tools -> Change Password* menu item. Refer to the following figure. You can type in your new password and set the time duration for which this password is to remain valid. Refer to the following figure.

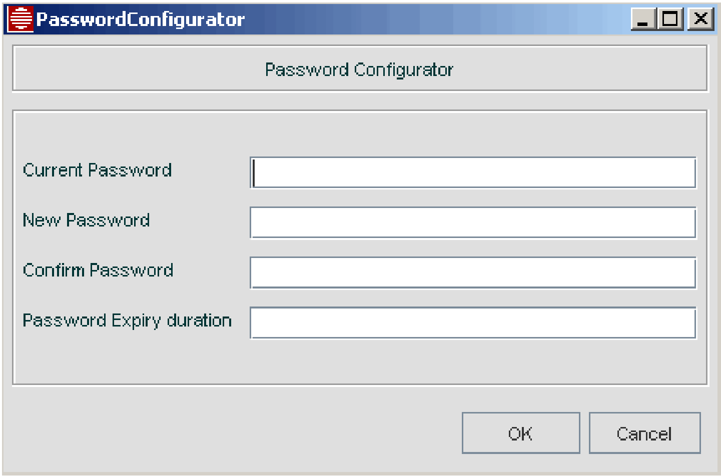


FIGURE 3-7 Setting a New Password

If at anytime you wish to change the password, select *Tools -> Change Password* from the main menu bar, and the **Password Configurator** form will reappear.

3.4.1 Configuration Limits for Clients

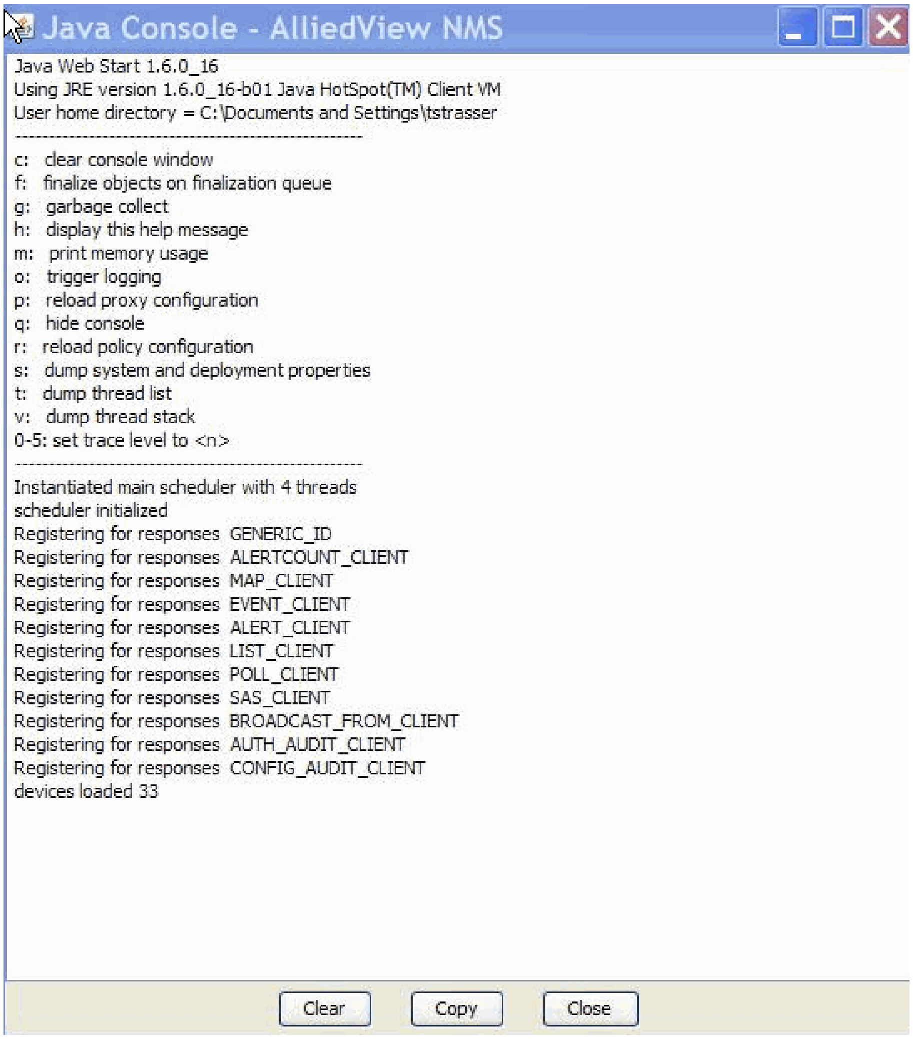
The AlliedView NMS server can support up to five GUI client connections at the same time. Connecting to the AlliedView NMS server using an HTML client counts as one of the five allowed users.

3.5 Using the Logs Console

When you start the client, you have the option of having a console file open during the session with AlliedView NMS. The console file tracks all events that occur between the client and server for the life of the session.

The following figure is an example of the console file when the client first starts. It includes general information about the AlliedView NMS configuration. Messages are grouped with a header for each day.

At any time during a session, the contents can be written to a file (**Save to File**) for archiving. Allied Telesis technical support may use the files for troubleshooting.

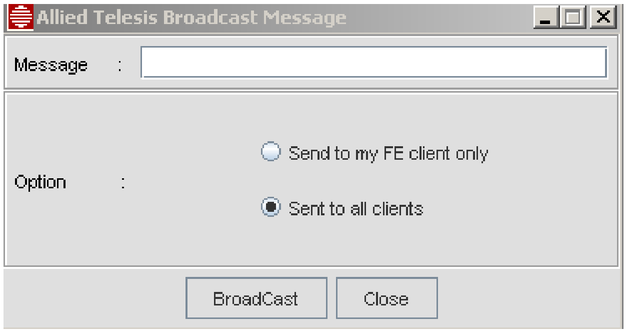


```
Java Web Start 1.6.0_16
Using JRE version 1.6.0_16-b01 Java HotSpot(TM) Client VM
User home directory = C:\Documents and Settings\tstrasser
----------------------------------------------------
c:   clear console window
f:   finalize objects on finalization queue
g:   garbage collect
h:   display this help message
m:   print memory usage
o:   trigger logging
p:   reload proxy configuration
q:   hide console
r:   reload policy configuration
s:   dump system and deployment properties
t:   dump thread list
v:   dump thread stack
0-5: set trace level to <n>
----------------------------------------------------
Instantiated main scheduler with 4 threads
scheduler initialized
Registering for responses  GENERIC_ID
Registering for responses  ALERTCOUNT_CLIENT
Registering for responses  MAP_CLIENT
Registering for responses  EVENT_CLIENT
Registering for responses  ALERT_CLIENT
Registering for responses  LIST_CLIENT
Registering for responses  POLL_CLIENT
Registering for responses  SAS_CLIENT
Registering for responses  BROADCAST_FROM_CLIENT
Registering for responses  AUTH_AUDIT_CLIENT
Registering for responses  CONFIG_AUDIT_CLIENT
devices loaded 33
```

FIGURE 3-8 Console File Window

3.6 Broadcasting a Message

The option *File -> Broadcast Message* can be used to send messages to all the clients. When this option is selected, the message is sent to all the clients managed by the main AlliedView NMS Server by default. (The option chosen does not matter.) When this option is selected, a dialog that contains the following details pops up. Refer to the following figure.



Message :

Option : ○ Send to my FE client only ● Sent to all clients

FIGURE 3-9 Broadcasting a Message (use bottom option only)

The following table lists the properties for broadcasting a message.

TABLE 3-4 Properties for Broadcasting a Message

Property	Details for Broadcast Message Properties
Message	The message to be broadcast.
Option	Two message options. The option **Send to my FE client only** is not supported. The other option is **Send to all clients**. When this option is selected, the message is sent to all the clients that are managed by the main AlliedView NMS Back-End Server.
BroadCast	Sends the message. The message sent is displayed in the status bar of the receiver.

3.7 Restart / Shut Down the Server

The procedures in this Guide that involve changes made to the server and its files do not need a server restart to take effect. You should restart the server only if a procedure instructs you to do so.

Warning: The administrator should avoid restarting the server, since during restart the AlliedView NMS is no longer monitoring devices and cannot communicate with any clients.

3.8 Resource Management

3.8.1 Setting the Custom Security Policy (Required)

This must be set for the server.

- Find the java runtime environment (jre). It's usually located in:

  <drive>:/Program Files/Java/jre*

  or use the Control Panel Java Plug-in tool "Advanced" tab to see the exact path of the java runtime.
- Open the java.policy file in lib/security (under the jre path).
- Append a tag for the NMS server in the system, as follows, where <server_name> is a host name or IP address:

  ```
  grant {
    permission java.net.SocketPermission "<server_name>", "accept,connect,resolve";
    permission java.awt.AWTPermission "setAppletStub";
  };
  ```
- Save the file.

Wildcard (*) can be used in the server_name but the wildcard must be the first character, such as *.sun.com.

You can combine the NMS-specific permissions for the server into a single grant, as follows:

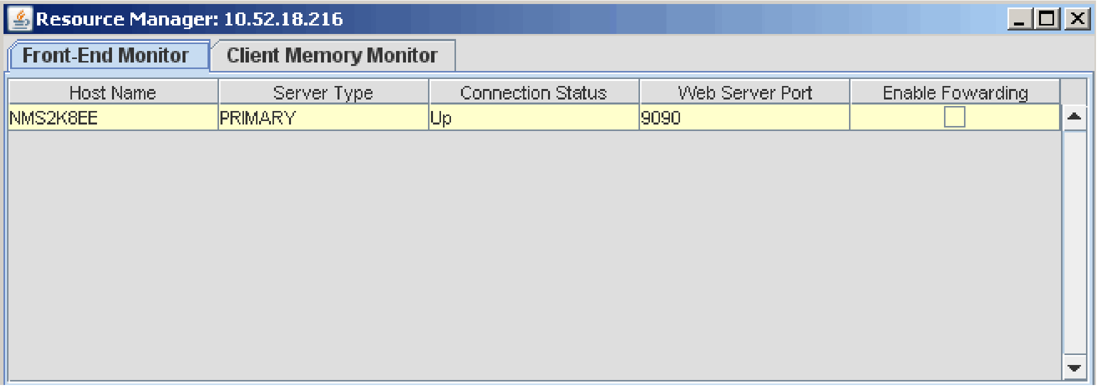
```
grant {
  permission java.net.SocketPermission "nmstest2", "accept,connect,resolve";
  permission java.awt.AWTPermission "setAppletStub";
};
```

nmstest2 is an example server.

3.8.2 Resource Management Table (*Tools -> Resource Management*)

To view the status of the server configuration, the user selects *Tools -> Resource Management* from the main menu. The **Resource Management** window appears, as shown in the following figure.

Note: This table should only be used by the Administrator.



Host Name	Server Type	Connection Status	Web Server Port	Enable Fowarding
NMS2K8EE	PRIMARY	Up	9090	□

FIGURE 3-10 Resource Manager Window - Back End Only

3.8.3 Front-End Monitor

Note: This applies to the distributed FE system available prior to 11.0.

In the example above, there is the default client to BE configuration. This has the following information:

- Resource Manager (in window title) - This is the server the client currently is connected to. (If the client is locally connected to the server this will be localhost.)
- HostName - These are the servers currently deployed in the AlliedView NMS server configuration. In the default BE only configuration, there is only one server and therefore only one row.
- Server Type - The BE server will have PRIMARY as the server type, while the FE servers will have STANDALONE.
- Connection Status - Working connections are Up. If a server fails this will change to Down.
- Web Server Port - This is the port used by the client to connect to the server.
- Enable Forwarding - This box is editable only when there is more than one server, and can only be activated for the FE server when the client is connected to that FE server. The feature is explained above.

3.8.4 Client Memory Monitor

This tab brings up a graph that monitors the memory used on the client. Memory allocated is the java heap space pre-allocated at start-up, while the used memory is the actual memory used by the client. If the client is functioning slowly, this graph can help determine if client memory usage is an issue. Refer to the following figure.

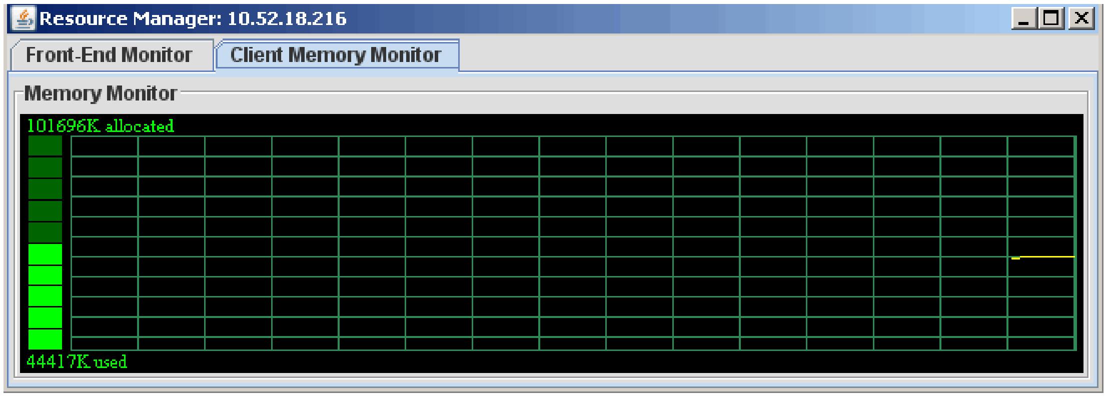


FIGURE 3-11 Client Memory Monitor

3.9 CPE Traps

To reduce unnecessary noise in the system, the NMS drops all incoming SNMP traps from CPE devices. To turn on CPE trap processing you must modify a properties file.

To turn on CPE trap processing:

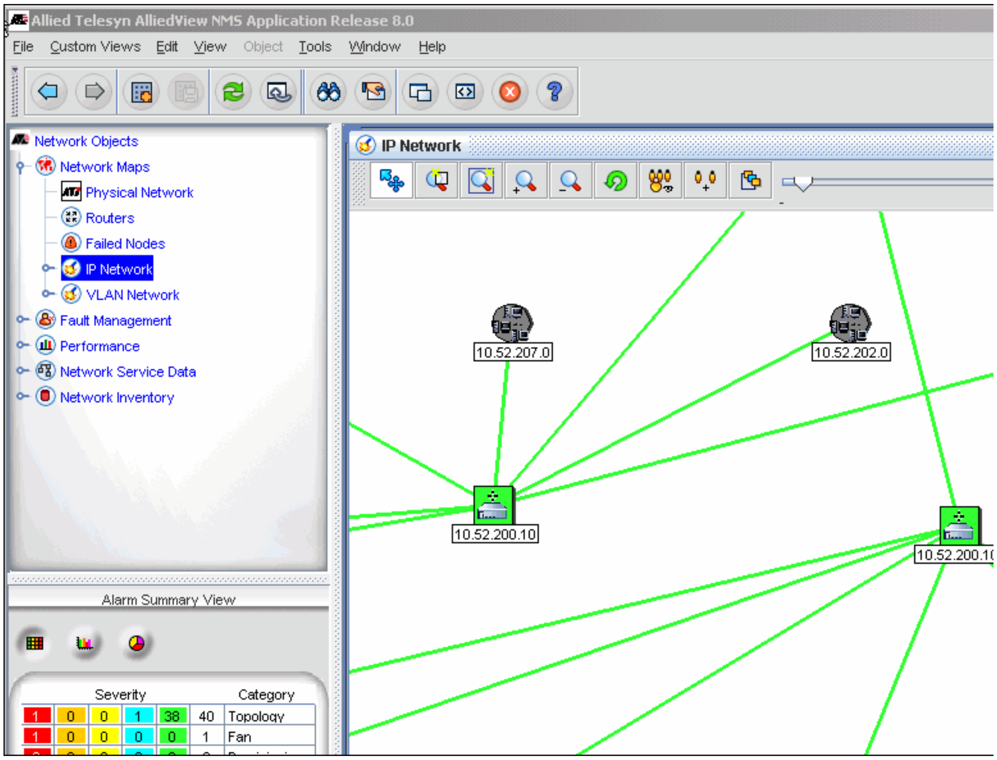
1. Open the file **<NMS_HOME>/conf/AT_trapControl.properties** in a text editor.

   <NMS_HOME> is the directory where the NMS is installed. The default in the installation wizard is:

   - Windows Server 2003/2008, XP, 7 (32-bit OS) - **c:\Program Files\Allied Telesis\AlliedView NMS**
   - Windows Server 2003/2008, XP, 7 (64-bit OS) - **c:\Program Files (x86)\Allied Telesis\AlliedView NMS**
   - Linux - **/opt/AlliedTelesis/AlliedViewNMS**
2. Change the parameter DROP_CPE_TRAPS = TRUE to DROP_CPE_TRAPS = FALSE.
3. Save the file.
4. Restart the NMS server. You must restart the server for changes to take effect.

4. Using the Network Maps

A Network Map is a graphical representation of networks and Network Elements (devices). Network elements, such as desktops, workstations, storage devices, servers, notebooks, printers, switches, routers etc., which are connected in a network, can be represented pictorially in a map. This ability of maps to expose logical relationships between devices and to show small but significant changes in the state of the Managed Objects (MOs), combined with showing complex networks, make maps an important component of NMS. The map panel consists of a background image and map symbols, which are representations of the managed objects. An example is shown in the following figure.



Severity						Category
1	0	0	1	38	40	Topology
1	0	0	0	0	1	Fan

FIGURE 4-1 Network Map Panel

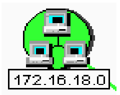
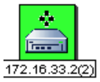
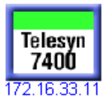
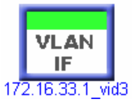
4.1 Accessing the Maps

The maps are accessed by clicking on the appropriate node in the network tree. When you click on a node, the map appears in the NMS Display Panel as shown in Figure 4-1. As the various maps are accessed, the panel-specific menu changes to reflect map-specific menu items. These menu items are described later in this section.

4.1.1 Understanding the Map Symbols and Colors

Each of the five default maps use symbols to represent various components of the network. These symbols and their meaning are shown in the following table.

TABLE 4-1 MAP Symbols

Symbol	Meaning
	This symbol represents a network in an Internet Protocol (IP) network or Virtual Local Area Network (VLAN).
	This symbol represents a router in a network.
———	This symbol is a solid line that interconnects objects on the map. It represents physical or logical connectivity between the two objects.
	This symbol represents a physical device on a network. The device type is reflected in the symbol table (e.g. iMAP 7400).
	This symbol represents a VLAN interface.
- - - - - - - -	This symbol is a dashed line that interconnects two VLAN interfaces in a VLAN. It represents logical connectivity between the two VLAN interfaces (VLAN IFs).

Each symbol on a map depicts the state of the associated component with one of six colors. Each of these colors and its meaning are listed in Table 3-3. Notice that all of the symbols shown in Table 4-1 reflect a no alarm state (green). Should some other condition exist, the green shown in the affected symbol will be replaced with an appropriate color from Table 3-3.

4.1.2 Using the Map Toolbar

The Toolbar specific to the map module is required for performing operations that are specific to maps and their display components. The Map Toolbar is displayed at the top of the right side panel of the selected map. Refer to the following figure.

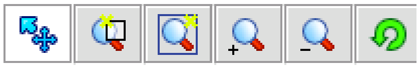


FIGURE 4-2 Map Toolbar

The Map Toolbar icons and their descriptions are given in the following table.

TABLE 4-2 Map Toolbar Icons

Toolbar Option	Icon	Description for Toolbar Icons
Select Mode	✥	Enables or disables select for objects on the map. When enabled (icon background is white), objects on the map can be selected. When disabled (icon background is gray), objects on the map cannot be selected.
Zoom Overview Window	🔍	Displays the **Zoom Overview** window. You can select a particular map symbol and click the Zoom Window tool of the Toolbar. The **Zoom Overview** window pops up displaying the exact location of the selected map symbol in the map view. This option is very useful when there are thousands of map symbols displayed in the map view, wherein you can find the exact location of the map symbol.
Zoom Mode	🔍	Enables you to select one or more map symbols for zooming. This is used for specific viewing of Map Symbols.
Zoom In	🔍+	Enlarges the view of the selected map. The selected map gets zoomed at the center.
Zoom Out	🔍−	Reduces the view of the selected map that has been zoomed in. With every click on the tool, the map retracts by one size.
Undo	↺	Undoes a performed action. That is, if an action, like deleting a map symbol, is performed then you can retrieve the symbol in the map by clicking this tool.

4.1.3 Using the Panel-Specific Menu for Maps

When a Network Map is accessed, menu items appear in the Panel-Specific Menu Bar that are specific to maps. Some of the items are common to all Network Maps, while others are specific to individual maps. The items common to all Network Maps include:

- *Custom Views* - Provides the means to create and modify maps. The items include:
  - *Add New Map* - Allows you to add a custom map
  - *Delete Map* - Deletes a map
  - *Relayout Map* - Restores the layout of the map symbols to the original positions
  - *Save Map* - Saves the map information to a file
- *Edit* - Provides map editing functions. The items include:
  - *Undo Add/Delete* - Removes the previously added item or restores the previously deleted item
  - *Clear Alarms* - Clears the alarms on a selected object
  - *Delete Alarms* - Deletes the alarms associated with a selected item
  - *Order By* - Sorts the objects on the map based on specific criteria
  - *Select All* - Selects all objects on a map
  - *Search* - Searches a map for specific information
- *View* - Provides access to information on a selected object. Items include:
  - *Details* - Displays the properties associated with a selected object
  - *Events* - Displays the events associated with a selected object
  - *Alarms* - Displays the alarms associated with a selected object
  - *Performance* - Displays the performance information associated with a selected object
  - *Refresh* - Refreshes the information for a selected object

The items specific to the individual maps are described later in this section.

4.1.4 Performing Common Tasks with the Maps

Use the following table to locate the task you wish to perform. If you are using NMS, use the screen or form name as well to locate the relevant section.

TABLE 4-3 Task List for the Map

Task	Screen /Form Name (if Applicable)	Section
Using the Physical Network map	Not applicable (n/a)	("Physical Network Map" on page 57)
Using the Routers map	n/a	("Routers Map" on page 58)
Using the Failed Nodes map	n/a	("Failed Nodes Map" on page 60)
Using the IP Network map	n/a	("IP Network Map" on page 60)
Using the VLAN Network map	n/a	("VLAN Network Map" on page 62)
Searching in a Map	n/a	("Searching for Elements in a Map" on page 65)
Sorting Map Symbols	n/a	("Sorting Map Symbols" on page 64)
Searching for Elements	Search	("Searching for Elements in a Map" on page 65)
Accessing Devices	iMAP Object Properties	("Accessing Devices (Managed Object Properties)" on page 65)
Map Properties	iMAP Map Properties	("Link Properties" on page 68)
Link Properties	iMAP Object Properties	("Link Properties" on page 68)

4.2 The Default Maps

The default Network Maps include the following:

- Physical Network - Shows the physical interconnections in the network
- Routers - Shows the routers in the network and how they are interconnected
- Failed Nodes - Shows the nodes that currently have one or more failures
- IP Network - Shows the IP interconnections in the network
- VLAN Network - Shows the VLAN configurations in the network

Each of these maps is represented as a node under the Network Maps branch of the NMS Tree. A node can be added anywhere in the tree by specifying the parent node of the node to be added. The menu found in this panel for the parent and the child need not be the same. That is, the child can have either the same tree pop-up menu as that of the parent node or any other tree pop-up menus. This feature fulfills the *Any Node Anywhere* concept, where you can provide different types of node under a parent node.

Note: Most commonly you would place nodes where they matched the management area.

4.2.1 Physical Network Map

The Physical Network map shows the discovered devices and their physical connections. An example is shown in the following figure.

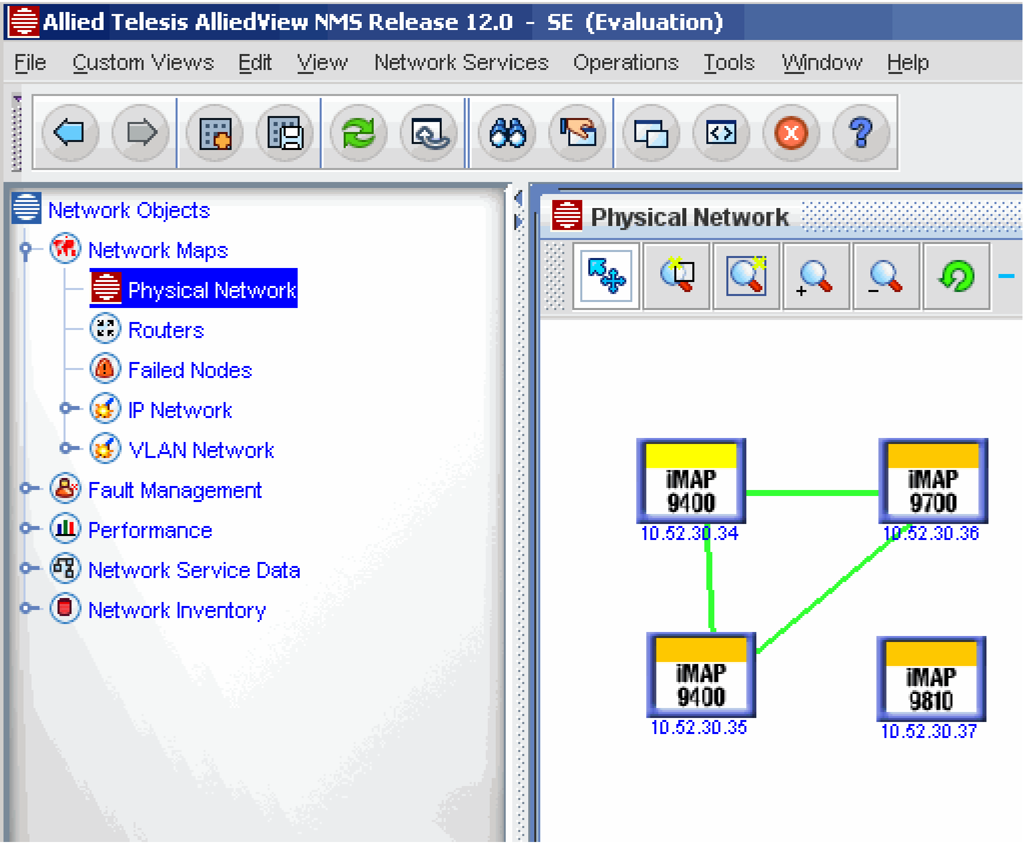


FIGURE 4-3 Example of a Physical Network Map

4.2.1.1 Physical Map Symbols

This map includes a physical device symbol for each discovered device. Each symbol includes the device type, a label, and a color, which represents the current criticality of the device. The physical connections are represented by a solid line on the map, which, in reality, may be one or more physical links. Since each line on the map may represent more than one physical link, the lines are referred to as link sets.

Note: Physical connections between devices must be manually specified so that they can show up as seen in Figure 4-3.

4.2.1.2 Physical Map Panel-Specific Menus

When the Network Map is selected, items appear on the Panel-Specific Menu Bar that are specific to the Physical Map. These items include:

- *Network Services* - Provides network link and VLAN functions initialized with selected node/link sets. Items include:
  - *Link Operations* - Provides the ability to add and delete Layer 2 links.
  - *Create Unmanaged Link Line* - Creates a symbolic link between two selected nodes.
  - *Audit CES Circuits*
  - *VLAN* - Provides show, create, and delete functions for VLANs, and provides access to the Network VLAN Manager.
  - *QoS* - Create QoS policies that will be applied to ports.

  - *Profile Menu* - Create Profiles for devices, ports, and iMG/RGs.
- *Operations* - Appears only when one or more network devices are selected and when a network object is right-clicked. It provides operational functions on the selected device or devices. Items include:
  - *View Chassis* - Displays the current chassis view for the selected device
  - *View Device Log* - Show in table format the logs for a selected device.
  - *Provision* - Provides provisioning functions for the selected device
  - *Network Services* - Provides network link and VLAN functions for the selected device
  - *Alarms/Events* - Displays the alarms or events, or a summary of the alarms and events for the selected device
  - *Performance* - Displays the performance information for the selected device
  - *View Config Comparison* - Brings up a tool to compare two config files.
  - *Discover Attached iMG/RGs* - Run discovery for the iMGs/RGs connected to the device ports.
  - *Display Switch FDB* - Displays the Forwarding Database for the selected device.
  - *PoE Management* - Displays power usage for devices with cards that support PoE.
  - *Port Authentication Management* - Displays port authentication and Radius settings for the device.
  - *Telnet To Device* - Opens a Telnet session to the selected device.
  - *SSH to Device* - Opens an SSH session to the selected device.
  - *Browse Device* - Opens a window to login to the device using its IP address. After entering an id and password, an interface (using html and javascript) opens, and allows local configuration, monitoring, managing, and diagnosing of the device.
  - *Rediscover Device* - Re-initiates discovery for the selected device
  - *Managed Object Properties* - Displays the MO properties for the selected device
  - *UnManage/Manage* - Sets the device to unmanaged if it is currently managed, or managed if it is currently unmanaged
  - *Update Status* - Updates the information on the selected device
- *Physical Link* - Appears only when one or more link sets are selected and when a link set is right-clicked. It provides operations and information on the selected link set or link sets. The items include:
  - *Link Operations* - Provides network link functions on the selected link set
  - *Show VLANs* - Displays all of the VLANs that are connected via the selected link set
  - *Link Alarm Events* - Display the alarms or events for the selected link
  - *Properties* - Displays the map symbol properties for the selected link set
  - *Managed Object Properties* - Displays the Managed Object Properties form for the selected link set
  - *UnManage/Manage* - Sets the link set to unmanaged if it is currently managed, or managed if it is currently unmanaged
  - *Update Status* - Updates the information on the selected device/links.

4.2.2 Routers Map

The Routers map displays all of the discovered routers on the network. An example is shown in the following figure.

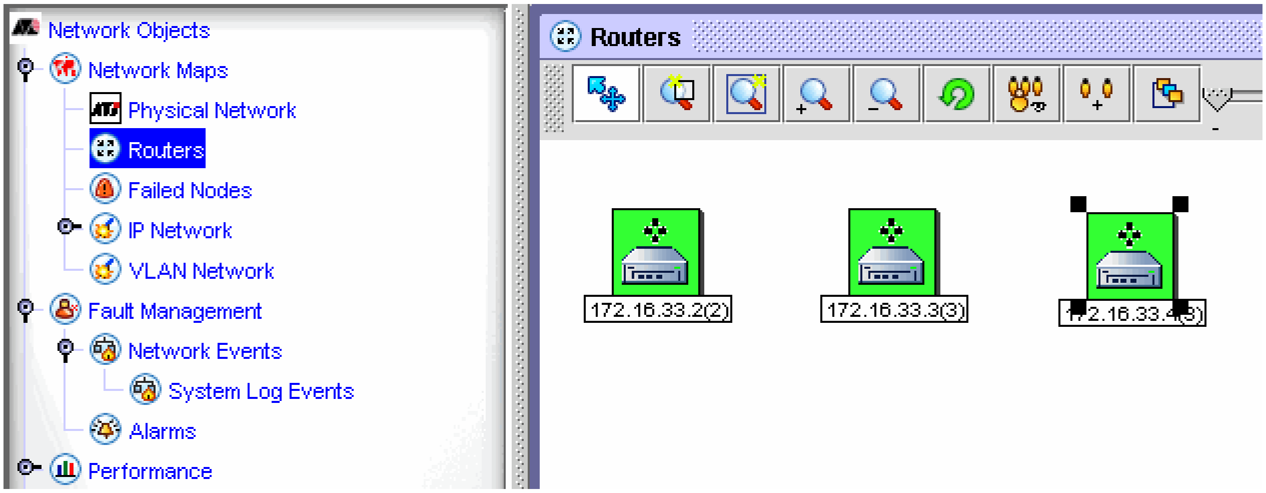


FIGURE 4-4 Example of the Routers Map

4.2.2.1 Router Map Symbols

The Router Map displays one router symbol for each discovered router. Each symbol has a label that identifies the router and a color that represents the current criticality of the router.

4.2.2.2 Router Map Panel-Specific Menus

When the Router Map is accessed, the *Router* menu appears on the Panel-Specific Menu Bar when one or more routers on the map are selected. The *Router* menu is also displayed when a router object is right-clicked. The *Router* menu provides various functions on the selected router or routers. The items on this menu include:

- *Router Details* - Displays the **Router Display Panel** for the selected router
- *Symbol Properties* - Displays the Symbol Properties form for the selected router
- *Managed Object Properties* - Displays the Managed Object Properties form for the selected router
- *Node Edit* - Provides the means to delete the symbol from the map or add/delete properties for the selected router
- *Delete Object and Traces* - Deletes the selected router from the map
- *Routing Table* - Displays the router table for the selected router
- *Interfaces* - Displays the interfaces for the selected router
- *TCP Table* - Displays the Transmission Control Protocol (TCP) table for the selected router
- *UDP Table* - Displays the User Datagram Protocol (UDP) table for the selected router
- *IpNetToMedia Table* - Displays the IP network to media table for the selected router
- *RMON Tables* - Displays the Remote Monitor (RMON) tables for the selected router
- *Events And Alarms* - Displays the alarms and events for the selected router
- *Telnet to device* - Initiates a Telnet session on the selected router
- *SnmpMonitor* - Starts the Simple Network Messaging Protocol (SNMP) monitor on the selected router
- *Performance* - Displays performance information for the selected router
- *Rediscover Device* - Re-initiates discovery for the selected device
- *UnManage/Manage* - Sets the link set to unmanaged if it is currently managed, or managed if it is currently unmanaged
- *Update Status* - Updates the status information on the selected router

4.2.3 Failed Nodes Map

The Failed Nodes map displays all nodes that have reported a major or critical failure. This map can be used to view all devices that are in such an alarm state. An example is shown in the following figure.

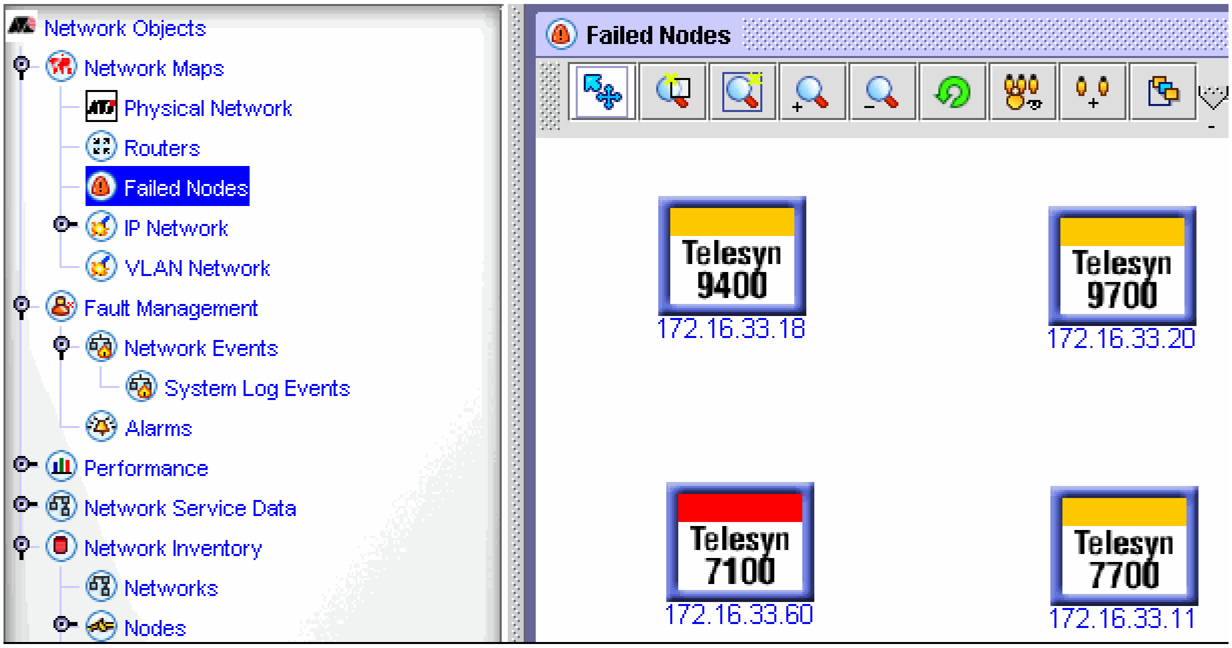


FIGURE 4-5 Failed Nodes

4.2.4 IP Network Map

The IP Network Map shows the configuration of the discovered IP networks. This map can be used to get a high-level view of the state of your networks. An example is shown in the following figure. Below the IP Network node in the NMS Tree may be one or more subnet maps. These maps narrow the view to a subnet. Clicking on any of the subnet map nodes will display a similar map for the selected subnet.

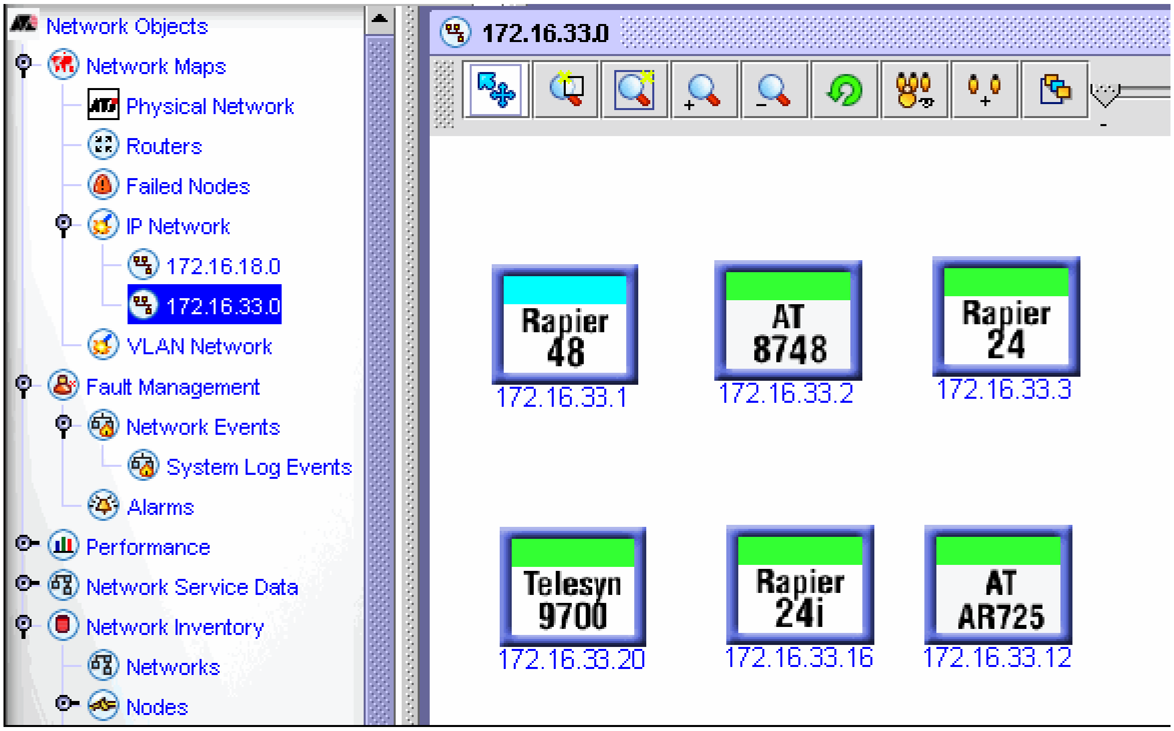


FIGURE 4-6 Example of the IP Network Map

4.2.4.1 IP Network Map Symbols

The IP Network Map uses the following symbols:

- Network - One symbol exists for each discovered network.
- Router - Represents a discovered router.
- Logical Connection - A solid line that interconnects the objects. Although identical in appearance to the physical connection symbol in the Physical Network map, this symbol represents a logical connection in the IP Network map and not a physical link set.

4.2.4.2 IP Network Panel-Specific Menus

When the IP Network map or one of its submaps is accessed, items appear in the Panel-Specific Menu Bar that are specific to IP Network maps. These menu items include:

- *Network* - Appears when one or more network objects are selected on the map or when a network icon is right-clicked. It performs various functions on the network object. The items include:
  - *Open Submap* - Displays the submap for the selected network
  - *Symbol Properties* - Displays the map symbol properties for the selected network
  - *Managed Object Properties* - Displays the Managed Object Properties form for the selected network
  - *Node Edit* - Provides the means to delete the symbol from the map or add/delete properties for the selected router
  - *Delete Object and Traces* - Deletes the select network object
  - *Stop Discovery* - Stops the discovery process for the selected network
  - *UnManage/Manage* - Sets the link set to unmanaged if it is currently managed, or managed if it is currently unmanaged
  - *Update Status* - Updates the status information for the selected network

- *Operations* - Appears when one or more router objects are selected or when a router object is right-clicked. This menu is the same as the *Operations* menu in the Router Map (refer to "Router Map Panel-Specific Menus" on page 59).
- *Linkmenu* - Appears when one or more link objects are selected or when a link is right-clicked. This menu provides access to information on the link. Items include:
  - *Properties* - Displays the map symbol properties for the selected link
  - *Managed Object Properties* - Displays the Managed Object Properties form for the selected link
  - *Delete Object and Traces* - Deletes the selected link
  - *Add/Delete Property* - Adds or deletes a property for the selected link
  - *UnManage/Manage* - Sets the link set to unmanaged if it is currently managed, or managed if it is currently unmanaged
  - *Update Status* - Updates the status information for the selected link

4.2.5 VLAN Network Map

The VLAN Network Map shows the configuration of discovered VLANs. This map can be used to get a high-level view of all the VLANs in your network and their Layer-3 (IP) connectivity. An example is shown in the following figure.

Note: To have a VLAN network map with links, these links must be already configured.

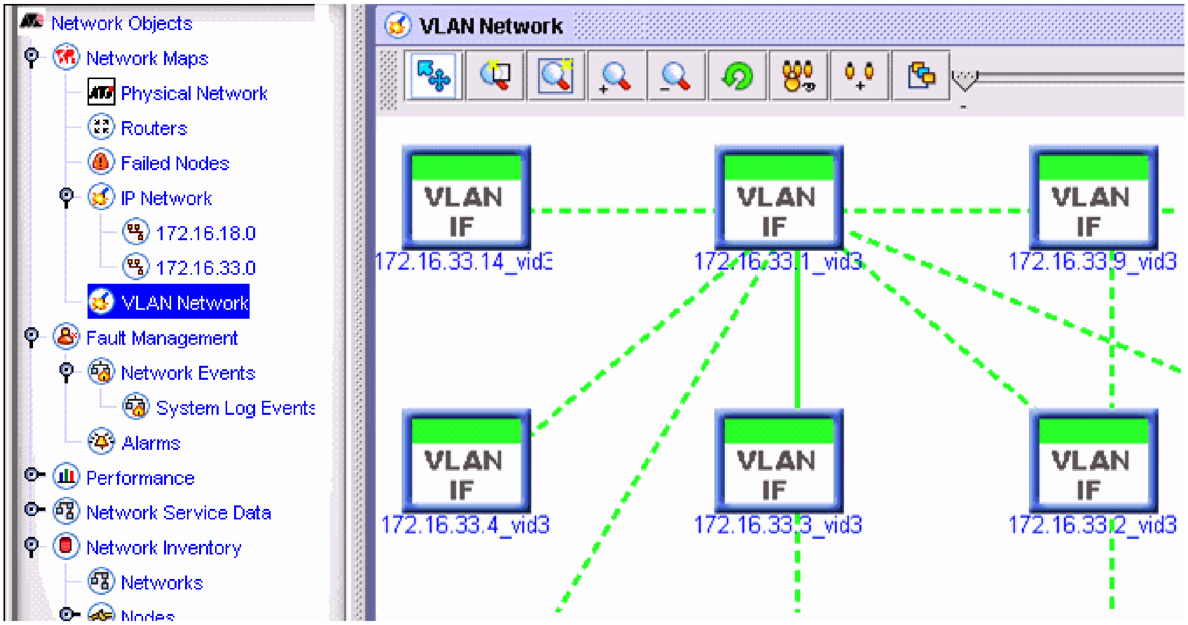


FIGURE 4-7 Example of the VLAN Network Map

Below the VLAN Network node in the NMS Tree may be one or more VLAN maps that show a single subnetwork or VLAN. These maps narrow the view to a specific Layer-2 subnetwork. Clicking on any of the VLAN map nodes will display a similar map for the selected VLAN.

4.2.5.1 VLAN Map Symbols

The VLAN Network map uses the same symbols as the IP Network map to show the VLAN configurations. These symbols include:

- Networks
- Routers
- Logical Connections (solid lines)

The VLAN Network submaps use the VLAN interface symbols and the VLAN connection symbols (dashed lines) to show VLAN configurations.

4.2.5.2 VLAN Network Panel-Specific Menus

When the VLAN Network map is accessed, items appear in the Panel-Specific Menu Bar that are specific to the VLAN Network map. These menu items include:

- *VlanNetwork* - Appears when one or more network objects are selected in the map. This menu provides functions on the VLAN networks. The menu items include:
  - *Open Submap* - Displays the submap for the selected network
  - *Symbol Properties* - Displays the map symbol properties for the selected network
  - *Managed Object Properties* - Displays the Managed Object Properties form for the selected network
  - *Alarms/Events* - Displays the alarms or events, or a summary of the alarms and events for the selected device
  - *UnManage/Manage* - Sets the link set to unmanaged if it is currently managed, or managed if it is currently unmanaged
  - *Update Status* - Updates the status information for the selected network
- *Operations* - Appears when one or more router objects are selected in the map. This menu is the same as the *Operations* menu in the IP Network map. Refer to "IP Network Panel-Specific Menus" on page 61.
- *Linkmenu* - Appears when one or more link objects are selected in the map. This menu is similar to the *Linkmenu* menu in the IP Network map. Refer to "IP Network Panel-Specific Menus" on page 61.

4.2.5.3 VLAN Network Submap Panel-Specific Menus

When a VLAN Network submap is accessed, items appear in the Panel-Specific Menu Bar that are specific to the VLAN Network submaps. These menu items include:

- *VLAN Operations* - Appears when a VLAN Network submap is displayed in the NMS Display Panel. This menu performs operations on VLANs and the VLAN submaps. The menu items include:
  - *Delete VLAN* - Deletes a VLAN.
  - *Map Properties* - Displays the Object Properties form for the map.
- *VLAN Interfaces* - Appears when one or more VLAN interface objects are selected on the map. This menu performs various operations on VLAN interfaces. The menu items include:
  - *Configure VLAN Interface* - Configures the selected VLAN interface.
  - *Extend Vlan* - Extends a VLAN.
  - *Managed Object Properties* - Displays the Managed Object Properties form for the selected VLAN interface.
  - *Alarms/Events* - Provides alarm and event information for the selected VLAN interface.
  - *UnManage/Manage* - Marks the selected interface as unmanaged if it currently is being managed, or as managed if it is currently unmanaged.
  - *Update Status* - Updates the status information on the selected VLAN interface.
- *VLAN Link* - Appears when one or more VLAN logical connection objects are selected in the map. This menu provides various operations on the VLAN links. The items include:
  - *Delete Vlan Link* - Deletes the selected VLAN link.
  - *Properties* - Displays the Symbol Properties tab of the Object Properties form for the selected VLAN link.
  - *Managed Object Properties* - Displays the Managed Object Properties form for the selected VLAN link.
  - *UnManage/Manage* - Sets the link set to unmanaged if it is currently managed, or managed if it is currently unmanaged.
  - *Update Status* - Updates the status information for the selected network.

4.3 Custom Views

Refer to Managed Object Properties and Custom Views for a list of properties that are commonly used to create meaningful custom views.

4.4 Using the Network Maps and Symbols

4.4.1 Sorting Map Symbols

To arrange the map symbols and facilitate the viewing of map symbols in maps, you can use the sort option. To sort the map symbols, select *Edit->OrderBy* from the Panel-Specific Menu Bar, and then specify a criteria. You can sort the map symbols as you wish based on the criteria in the following table.

TABLE 4-4 Sorting Criteria for Map Symbols

Criteria for Sorting	Description for Sorting Criteria
name	Sorts the map symbols based on their *names*. Order of sorting is ascending American Standard Code for Information Interchange (ASCII).
label	Sorts the map symbols based on the symbols' *label* values. Order of sorting is ascending ASCII.
objName	Sorts the map symbols based on the name of the managed object that is represented by the symbol.
status	Sorts the map symbols based on the status of the managed objects represented by the symbols. Order of sorting is from *critical* to *clear,* meaning critical symbols will be positioned first followed by symbols of lower severity.
objType	Sorts the map symbols based on the type of the managed object represented by the symbols. (Node, Network, Router, Switch etc.)

Note: *The sorting of map symbols will not take place once you save the map. This is because sorting occurs only for the symbols whose anchor property is set to False. When you save a map, the anchor property of all symbols is set to True and so the sorting will not occur.*

4.4.2 Managing and Unmanaging Elements in the Map

Managing an element means that you are making the NMS monitor the element, while unmanaging an element means that you are making the NMS stop monitoring the element. Every object in the map has a symbolic representation of a network element, so the user can manage or unmanage elements as needed.

A selected map symbol can be made managed or unmanaged either by selecting the map symbol and then selecting the *Operations->Manage* or *Operations->UnManage* from the Panel-Specific Menu Bar, or by right-clicking the map symbol, and then selecting *Manage* or *UnManage*. The actual option selected will depend on whether the selected map symbol is currently in the managed or unmanaged state (it is a toggle operation).

Once a selected map symbol is made managed, you can find the icon displayed against the selected map symbol in the color that reflects the severity status of the device. The same icon becomes gray in color when the selected device is made unmanaged.

Note: *When the NMS has discovered an object (device) but it is not yet being managed (monitored), it will have a gray color. Double-clicking the device will cause the message No Data to appear in the console. Since the device has been discovered, selecting the Network->Manage from the Panel-Specific Menu Bar will load the data and change the device color to reflect the device severity status.*

4.4.3 Drilling Down

Drilling down into a network means exploring the details of a network element displayed in a map. Each displayed network element is represented by a network icon in the displayed map. The network layout of this network element gets displayed as a submap by double-clicking the corresponding network icon. In this way, you can retrieve the information of all the elements of the sub networks, which are represented pictorially in the sub maps. The displayed map may contain certain sub maps of the displayed networks.

4.4.4 Searching for Elements in a Map

You can search for elements in a map based on certain match criteria. For example, you can search all elements displayed in the current map based on the element's label name. This section describes how you should go about searching for an element in a map. The search is made on all the elements in the current map displayed on the interface.

The search option can be invoked by selecting *Edit->Search* from the Menu-Specific Menu Bar, or by clicking the **Find** button ( ) in the Toolbar. The result is the following figure.

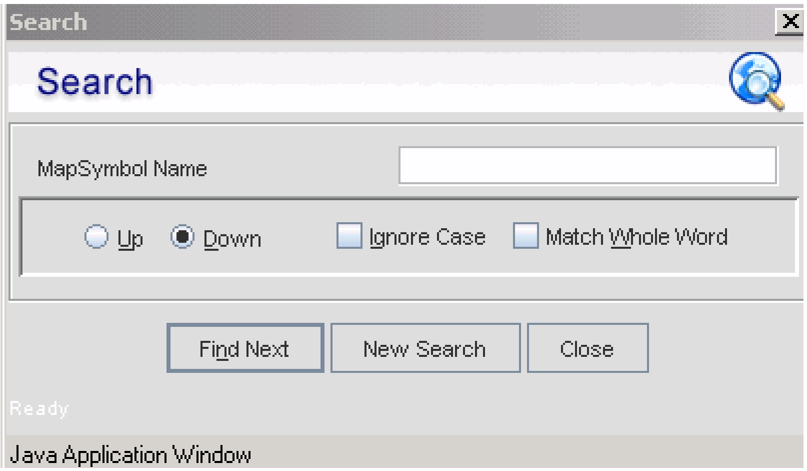


FIGURE 4-8 Find/Search Form

In the **Find** form, enter the label name in the **Symbol label** text field available in the search screen and click **Find next**. You can skip a particular map by choosing the **Next map** button, which moves to the next map available in the NMS Tree.

The **Up** and **Down** radio buttons can be used to notify the direction in which the search is to be performed. To search for an element in a map, you can also use the **Ignore case** option and the **Match whole word** option for an easy search. The **New search** button resets the values on the search form to the defaults. The **Close** button closes the search window, and the **Help** button displays the help document *Searching for Elements in Map Views.*

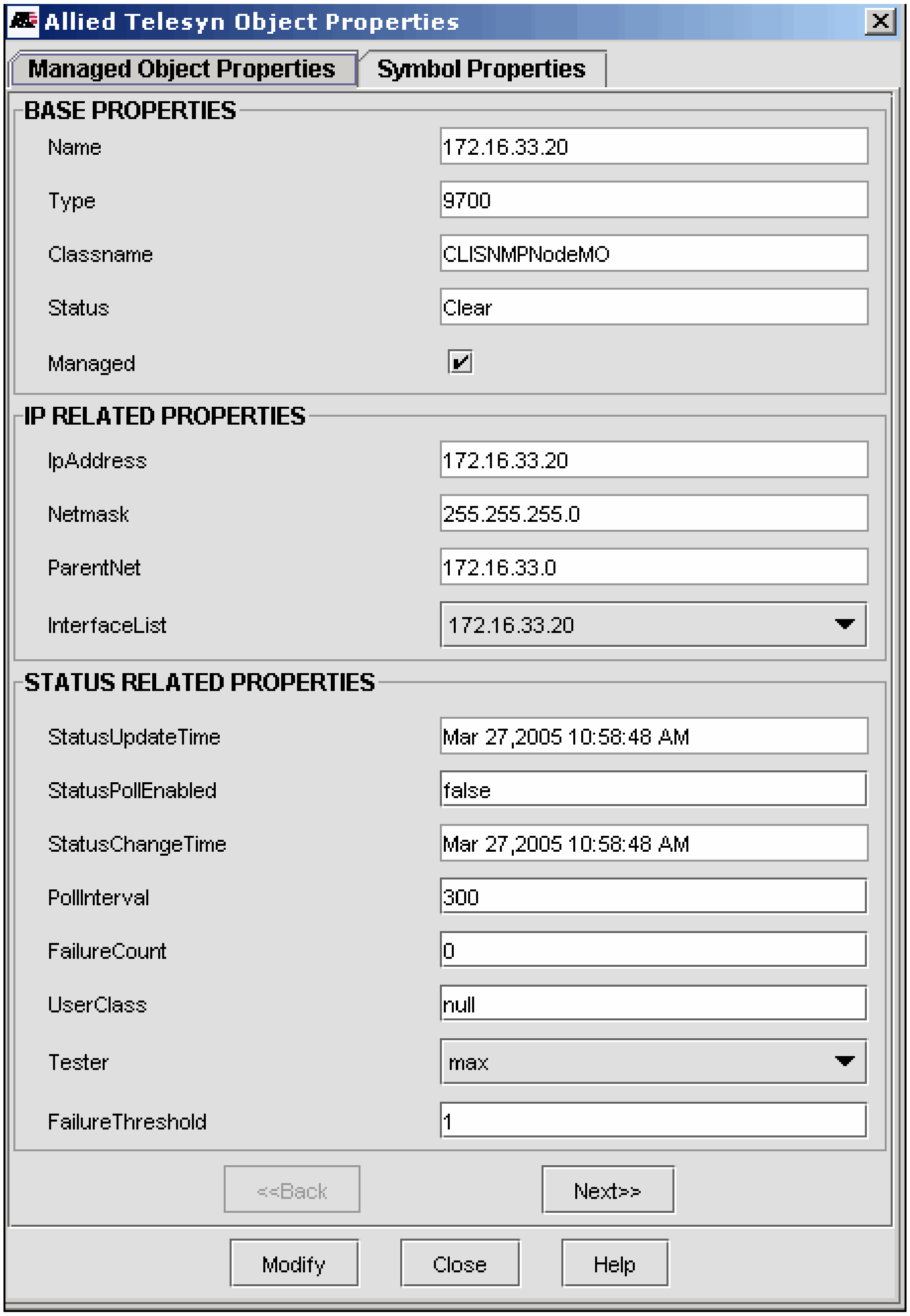
4.4.5 Accessing Devices (Managed Object Properties)

When a network is discovered, all the devices that are discovered in that network are represented as symbols in the submap associated with each network. When devices are discovered, their symbols are added to the submap. Each device has properties associated with it. The property details of every device that has been discovered can be viewed by displaying the device Object Properties form.

The Object Property form is a tabbed panel that contains the tabs **Managed Object Properties** and **Symbol Properties**. The details, such as a description of the element status, the device name, the display name, the device status, whether the device is managed or not, etc., are given in the Object Properties form. You can access the device Object Property form by clicking its symbol, and then selecting *View -> Details* from the Panel-Specific Menu Bar, or by right-clicking the device symbol, and then and selecting the *Managed Object Properties* option.

The Object Property form is the same for all network elements. The following figure shows a sample Object Properties form.

Note: For a complete list of MO attributes and examples, refer to Object Properties to Define Objects and Custom Views.



BASE PROPERTIES

Name	172.16.33.20
Type	9700
Classname	CLISNMPNodeMO
Status	Clear
Managed	☑

IP RELATED PROPERTIES

IpAddress	172.16.33.20
Netmask	255.255.255.0
ParentNet	172.16.33.0
InterfaceList	172.16.33.20

STATUS RELATED PROPERTIES

StatusUpdateTime	Mar 27,2005 10:58:48 AM
StatusPollEnabled	false
StatusChangeTime	Mar 27,2005 10:58:48 AM
PollInterval	300
FailureCount	0
UserClass	null
Tester	max
FailureThreshold	1

FIGURE 4-9 Object Properties Form

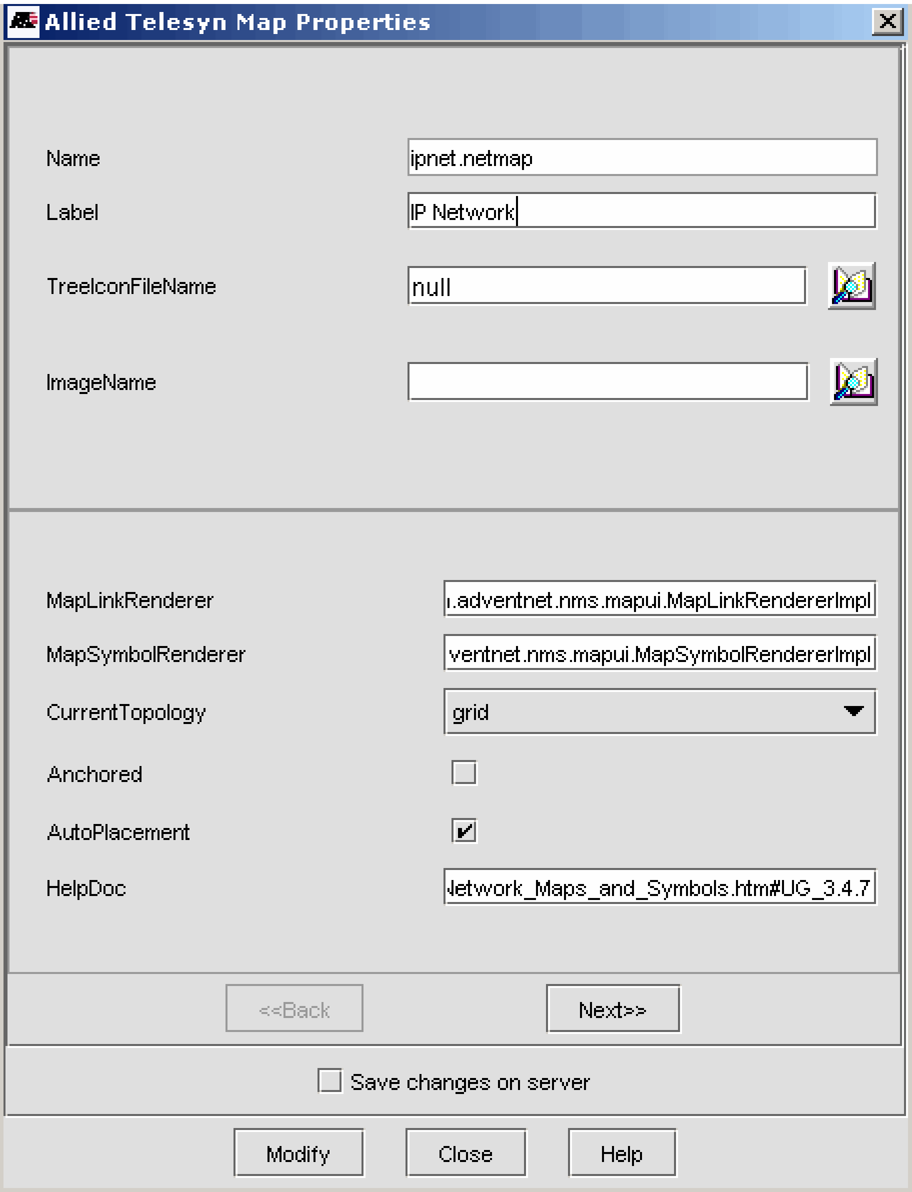
Note: The communication and inventory details (placed together as Advanced Device Information) of the discovered devices can also be accessed. All these details are given as tables. The tabular information derived from the SNMP Agents associated with these devices is defined in the RFC 1213 MIB, Bridge-MIB, and in the Printer MIB. These details are presented in Advanced Device Information in this guide. The advanced device information details how the packets traverse in a network.

The **Managed Object Properties** fields can be entered in both the map view and the Network Inventory view.

4.4.6 Viewing Map and Symbol Properties

4.4.6.1 Map Properties

The Map Properties form contains the map properties, such as its name, label, image name, etc. The details can be viewed and modified, if necessary, by double-clicking on the map or by selecting *View->Details* from the Panel-Specific Menu Bar when no objects on the map are selected. The various map properties that are displayed are shown in the following figure.



Allied Telesyn Map Properties

Name	ipnet.netmap
Label	IP Network
TreeIconFileName	null
ImageName	
MapLinkRenderer	ı.adventnet.nms.mapui.MapLinkRendererImpl
MapSymbolRenderer	ventnet.nms.mapui.MapSymbolRendererImpl
CurrentTopology	grid
Anchored	□
AutoPlacement	☑
HelpDoc	letwork_Maps_and_Symbols.htm#UG_3.4.7

FIGURE 4-10 Map Symbol Properties Form

The following table lists the map properties while the next table lists the map criteria properties that appear after clicking Next on the properties form.

TABLE 4-5 Map Properties

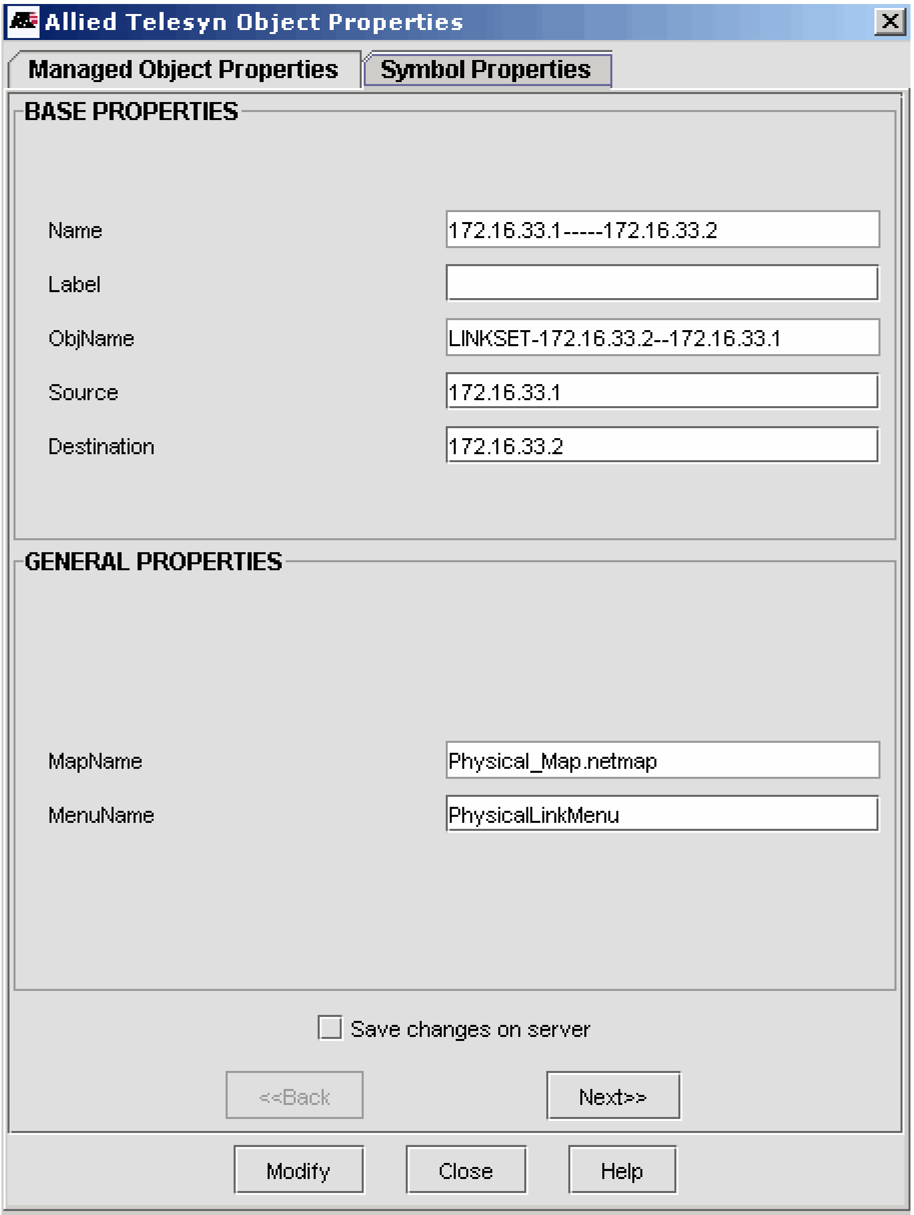
Property	Description for Map properties
Name	The unique name of the map, which is non-editable.
Label	The label of the map, which is displayed in the tree.
TreeIconFileName	The icon that is to represent the map in the tree.
ImageName	The image that appears as the background of the map.
MapLinkRenderer	The name of the renderer for the links placed in the map.
MapSymbolRenderer	The name of the renderer for the symbols placed in the map.
CurrentTopology	The name of the renderer for the symbols placed in the map.
Anchored	A checkbox that specifies whether the map symbols are anchored. If checked, the user cannot edit, cut, or copy any map symbols, links, etc.
AutoPlacement	A checkbox that specifies whether the map symbols are to be placed automatically. If checked, the symbols are placed automatically.
HelpDoc	The URL of the help document to be invoked for the help option of this map.

TABLE 4-6 Map Criteria Properties

Property	Description for Map Criteria Properties
MenuName	The panel-specific menu configuration file

4.4.6.2 Link Properties

Links represent the connection between two objects. The Object Properties form consists of properties such as name, label, source, destination, etc. It also contains the object-related properties and the user-related properties. The following figure shows a sample Object Properties form for a link.



Name	172.16.33.1-----172.16.33.2
Label	
ObjName	LINKSET-172.16.33.2--172.16.33.1
Source	172.16.33.1
Destination	172.16.33.2
MapName	Physical_Map.netmap
MenuName	PhysicalLinkMenu

☐ Save changes on server

f

FIGURE 4-11 Link Symbol Properties Form

The Symbol Properties tab in the Object Properties form are shown in the following table.

TABLE 4-7 Symbol Properties for Links

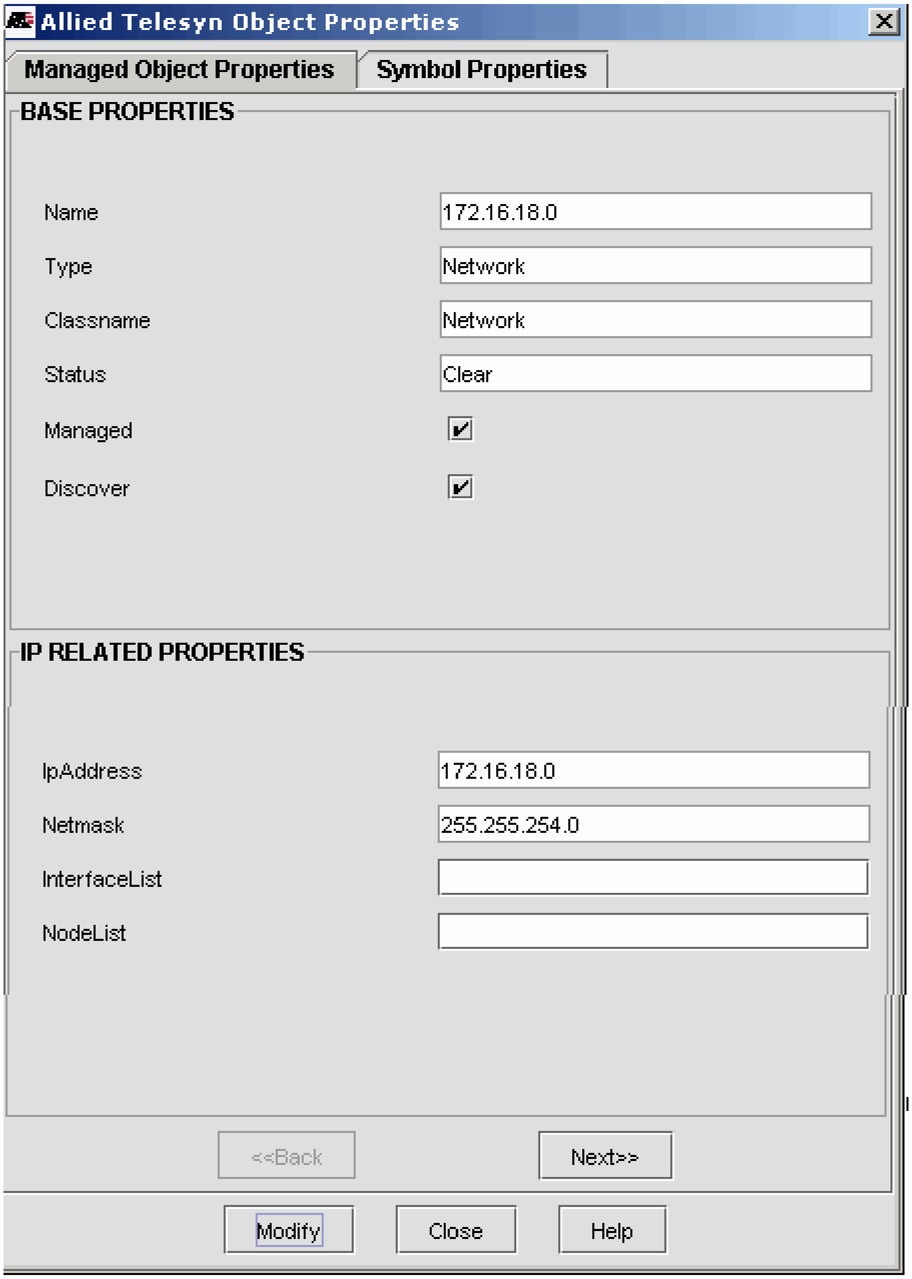
Property	Symbol Property for Links
Name	A unique name for the map link. This property cannot be edited.
Label	The label of the map link.
ObjName	The name of the managed object with which the map link is associated.
Source	The name of the starting map symbol from where the link starts.
Destination	The name of the destination map symbol where the link ends.
MapName	The name of the map on which the link is placed. This property cannot be edited.

TABLE 4-7 Symbol Properties for Links (Continued)

Property	Symbol Property for Links
MenuName	The name of the object-specific menu configuration file.
ObjType	The type of the managed object from the combo box.
LinkType	The type of link that is to be rendered in the map. That is, based on the value specified for the LinkType, the desired type of link can be rendered in the map.
Status	The severity of the symbol is mentioned here. This property cannot be edited.
Managed	A checkbox that indicates whether the object is managed by the NMS. If checked, the object is managed.
Thickness	The thickness of the link line.
OwnerName	The name of the owner to whom the link belongs.
Type	The type of the link.
iconName	The name of the icon that is to represent the link in the Network Inventory.
X	The X coordinate value of the position of the Map Link.
Y	The Y coordinate value of the position of the Map Link.
ParentName	The name of the parent in the NMS Tree.
Anchored	A boolean that indicates whether the object is anchored on the map. If set to true, the object is anchored.

4.4.6.3 Network Object Properties

The Object Properties form that is displayed for network objects includes symbol and managed object properties. The following figure shows a sample Symbol Properties form for a network symbol.



BASE PROPERTIES

Name	172.16.18.0
Type	Network
Classname	Network
Status	Clear
Managed	☑
Discover	☑

IP RELATED PROPERTIES

IpAddress	172.16.18.0
Netmask	255.255.254.0
InterfaceList	
NodeList	

FIGURE 4-12 Network Symbol Properties Form

The following table lists the Symbol Properties for network objects.

TABLE 4-8 Symbol Properties for Network Objects

Property	Symbol Properties for Network Objects
Name	A unique name for the map symbol. This property cannot be edited.
Label	The label of the map symbol.
ObjName	The name of the managed object for which the map symbol is added.
MapName	The name of the map on which the symbol is placed. This property cannot be edited.

TABLE 4-8 Symbol Properties for Network Objects

Property	Symbol Properties for Network Objects
IconName	The name of the icon that represents the map symbol.
MenuName	The name of the object-specific menu configuration file. You can change the menu file at run time.
ParentName	The name of the parent in the tree.
ObjType	The type of the managed object from the combo box.
Status	The severity of the symbol is mentioned here. This property cannot be edited.
Managed	A checkbox that sets the object to managed/unmanaged. When checked, the object is managed.
Discover	A checkbox that enables/disables object discovery. When checked, discovery is enabled.
Anchored	A checkbox that sets the object to anchored/unanchored. When checked, the object is anchored, which means the symbol is not handled by the map layout. For example, you can move the symbol anywhere in the layout. When you zoom in, it won't be in the moved position; that is, it remains in its original position.
X	The X coordinate value of the position of the map symbol.
Y	The Y coordinate value of the position of the map symbol.
Height	The height of the map symbol image.
Width	The width of the map symbol image.
OwnerName	The name of the object owner.
Type	The object type.

4.4.6.4 Container Object Properties

Containers are created in a map and contain different map symbols. The map symbol, whose container name is specified against the parentName property in the form, is encapsulated in a specific container. The following table lists the properties for containers.

TABLE 4-9 Container Object Properties

Property	Description for Container Properties
containment	A boolean that indicates whether the symbols inside the container should truly be contained within the boundaries of the container. If the value is set to True you cannot move any of the symbols outside the boundaries of the container (meaning containment is true). If it is set to False you can move symbols outside the boundaries and still they will be children objects of the container with their ParentName referring to the container object.
layout	The layout of the map symbols that are contained in the container. You can change the layout as per your requirement.
currentlayout	The current layout of the map symbols of the container.

4.4.7 Monitoring and Controlling Devices

A Network Manager must be informed on the state of every device on the networks that he or she is monitoring. The Network Manager receives network notifications about the state of every managed device. These notifications are either unsolicited messages sent either by the agent in the device or through status polling techniques configured by the Administrator. These malfunctions or faults are acknowledged by the NMS as generated events and alarms. You can view the generated events and alarms for a MO by selecting the corresponding map symbol displayed in the map. This can be accomplished by selecting *View->Events* or *View->Alarms* from the Panel-Specific Menu Bar. On selecting the required menu item (i.e., *Events* or *Alarms*) from the Panel-Specific Menu Bar, the corresponding panel is displayed, which contains the generated events or alarms of the selected map symbol.

4.4.7.1 Accessing Alarms for Device

You can view the alarms generated for the MOs by selecting the corresponding map symbols displayed in the map and selecting *View->Alarms* from the Panel-Specific Menu Bar. On clicking this menu option, the Alarms panel (under Fault Management) of the NMS Tree gets selected, displaying the last generated alarm and its severity status for the selected map symbol.

You can also right-click on a device, and then select *Alarms/Events - > Alarms* from the pop-up menu.

4.4.7.2 Accessing Events

You can view the events generated for the MOs by selecting the corresponding map symbols displayed in the map and selecting *View->Events* from the Panel-Specific Menu Bar. On selecting this menu option, the Network Events panel (under Fault Management) of the NMS Tree is selected, displaying the list of generated events over a period of time for the selected map symbol.

You can also right-click on a device, and then select *Alarms/Events - > Events* or *Alarms/Events - > Summary* from the pop-up menu.

4.4.7.3 Accessing Statistics

You can retrieve polled data collected for the MOs by selecting the corresponding map symbols displayed in the map and selecting *View->Performance* from the Panel-Specific Menu Bar. Based on the collected statistical data, the performance of the selected device can be monitored for a given time period. On selecting this menu option, the Configured Collection panel (under Performance) of the NMS Tree is selected, displaying the created polled data for the selected map symbol.

You can also right click on a device, and then select *Performance* from the pop-up menu.

4.4.7.4 Updating Status

To poll an element for its status, you can right click on the element, and then select *Update Status* from the pop-up menu. This menu item enables the user to view the status of the selected map symbol despite the set polling period. You can also select the symbol on the map, and then select *Operations->Update Status* from the Panel-Specific Menu Bar.

5. Using the Network Inventory View

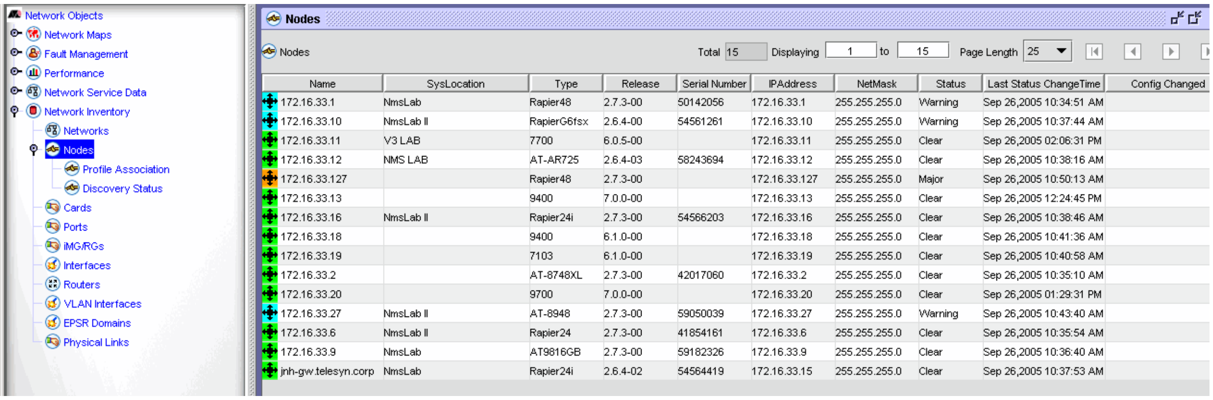
The Network Inventory view is used to view, search, modify, and delete network objects, such as networks, nodes, and interfaces. The Network Inventory view displays an inventory of all network entities, such as networks, nodes, ports, interfaces, routers, and links. Under the Network Inventory node in the NMS Tree are the following default subviews:

- Networks
- Nodes
  - Profile Association
  - Discovery Status
- Cards
- Ports
- iMG/RGs
- Interfaces
- Routers
- VLAN Interfaces
- EPSR Domains
- Physical Links

Each of these subviews narrows the network inventory to a specific type.

5.1 Network Inventory View

The Network Inventory maintains the properties of all MOs in a network. These MOs and their object properties are listed in the Network Inventory panel, as shown in the following figure.



Name	SysLocation	Type	Release	Serial Number	IPAddress	NetMask	Status	Last Status ChangeTime	Config Changed
172.16.33.1	NmsLab	Rapier48	2.7.3-00	50142056	172.16.33.1	255.255.255.0	Warning	Sep 26,2005 10:34:51 AM	
172.16.33.10	NmsLab II	RapierG6fsx	2.6.4-00	54561261	172.16.33.10	255.255.255.0	Warning	Sep 26,2005 10:37:44 AM	
172.16.33.11	V3 LAB	7700	6.0.5-00		172.16.33.11	255.255.255.0	Clear	Sep 26,2005 02:06:31 PM	
172.16.33.12	NMS LAB	AT-AR725	2.6.4-03	58243694	172.16.33.12	255.255.255.0	Clear	Sep 26,2005 10:38:16 AM	
172.16.33.127		Rapier48	2.7.3-00		172.16.33.127	255.255.255.0	Major	Sep 26,2005 10:50:13 AM	
172.16.33.13		9400	7.0.0-00		172.16.33.13	255.255.255.0	Clear	Sep 26,2005 12:24:45 PM	
172.16.33.16	NmsLab II	Rapier24i	2.7.3-00	54566203	172.16.33.16	255.255.255.0	Clear	Sep 26,2005 10:38:46 AM	
172.16.33.18		9400	6.1.0-00		172.16.33.18	255.255.255.0	Clear	Sep 26,2005 10:41:36 AM	
172.16.33.19		7103	6.1.0-00		172.16.33.19	255.255.255.0	Clear	Sep 26,2005 10:40:58 AM	
172.16.33.2		AT-8748XL	2.7.3-00	42017060	172.16.33.2	255.255.255.0	Clear	Sep 26,2005 10:35:10 AM	
172.16.33.20		9700	7.0.0-00		172.16.33.20	255.255.255.0	Clear	Sep 26,2005 01:29:31 PM	
172.16.33.27	NmsLab II	AT-8948	2.7.3-00	59050039	172.16.33.27	255.255.255.0	Warning	Sep 26,2005 10:43:40 AM	
172.16.33.6	NmsLab II	Rapier24	2.7.3-00	41854161	172.16.33.6	255.255.255.0	Clear	Sep 26,2005 10:35:54 AM	
172.16.33.9	NmsLab	AT9816GB	2.7.3-00	59182326	172.16.33.9	255.255.255.0	Clear	Sep 26,2005 10:36:40 AM	
jnh-gw.telesyn.corp	NmsLab	Rapier24i	2.6.4-02	54564419	172.16.33.15	255.255.255.0	Clear	Sep 26,2005 10:37:53 AM	

FIGURE 5-1 Network Inventory Main View

Refer to Navigating in a View for information on navigating the view. Refer to Searching in a View for information on searching the view.

When the Network Inventory view is displayed in the NMS Display Panel, items appear in the Panel-Specific Menu Bar that are specific to the Network Inventory views. Some of the items are specific to the type of object that is selected in the view, while others are common to all of the object types. The common items include:

- *Edit* - Provides editing functions for the view. Items include:
  - *Add Node* - Adds a node.
  - *Add Network* - Adds a network.
  - *Refresh Node* - Updates the information on the selected node.
  - *Clear Alarms* - Clears the alarms on the selected node.
  - *Delete Alarms* - Deletes from the alarm database the alarms on the selected node.
  - *Search* - Provides a search function for the view.
  - *Export Table Data* - Provides an export function for all of the view data. The data may be exported to a file (in delimited tabular form) or to a Web browser. The data may also be filtered.
  - *Export Selected Rows* - Provides an export function for selected rows in the view data.
- *View* - Displays additional information. Items include:
  - *Details* - Displays detailed information on the selected object.
  - *Events* - Opens a Network Events view in which the events associated with the selected object are displayed.
  - *Alarms* - Opens an Alarms view in which the alarms associated with the selected object are displayed.
  - *Performance* - Opens a Configured Collection view in which the statistics for the selected object are displayed.
  - *Refresh* - Updates the information on the selected object.

These menu items also appear for all of the Network View subviews. The object-type-specific menus include:

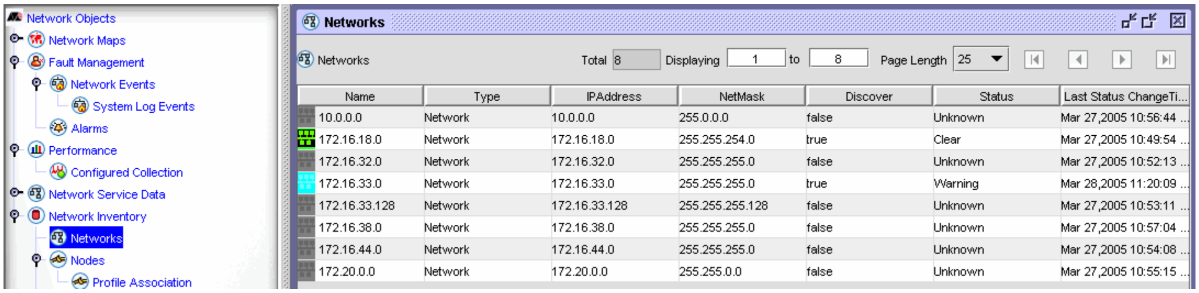
- *Network* - For network objects
- *Operations* - For nodes and routers on the network
- *Port* - For customer ports
- Interface - For Interfaces (This includes the Ping menu item.)
- *VLAN Interface* - For VLAN interface objects
- *Link* - For physical link objects

The object-type-specific menus are described in the following sections.

5.2 The Network Inventory Subviews

5.2.1 Networks Subview

The Networks subview narrows the Network Inventory view to the discovered network objects. To access this view, click on the Networks node under Network Inventory in the NMS Tree. An example is shown in the following figure.



Name	Type	IPAddress	NetMask	Discover	Status	Last Status ChangeTi...
10.0.0.0	Network	10.0.0.0	255.0.0.0	false	Unknown	Mar 27,2005 10:56:44 ...
172.16.18.0	Network	172.16.18.0	255.255.254.0	true	Clear	Mar 27,2005 10:49:54 ...
172.16.32.0	Network	172.16.32.0	255.255.255.0	false	Unknown	Mar 27,2005 10:52:13 ...
172.16.33.0	Network	172.16.33.0	255.255.255.0	true	Warning	Mar 28,2005 11:20:09 ...
172.16.33.128	Network	172.16.33.128	255.255.255.128	false	Unknown	Mar 27,2005 10:53:11 ...
172.16.38.0	Network	172.16.38.0	255.255.255.0	false	Unknown	Mar 27,2005 10:57:04 ...
172.16.44.0	Network	172.16.44.0	255.255.255.0	false	Unknown	Mar 27,2005 10:54:08 ...
172.20.0.0	Network	172.20.0.0	255.255.0.0	false	Unknown	Mar 27,2005 10:55:15 ...

FIGURE 5-2 Example Networks Subview

When the Networks subview is displayed in the Display Panel or when a network object is selected in the Network Inventory view, the *Network* menu appears in the Panel-Specific Menu Bar, which is specific to networks objects. In the Networks subview, the menu appears when you select an item in the view. The items in the *Network* menu include:

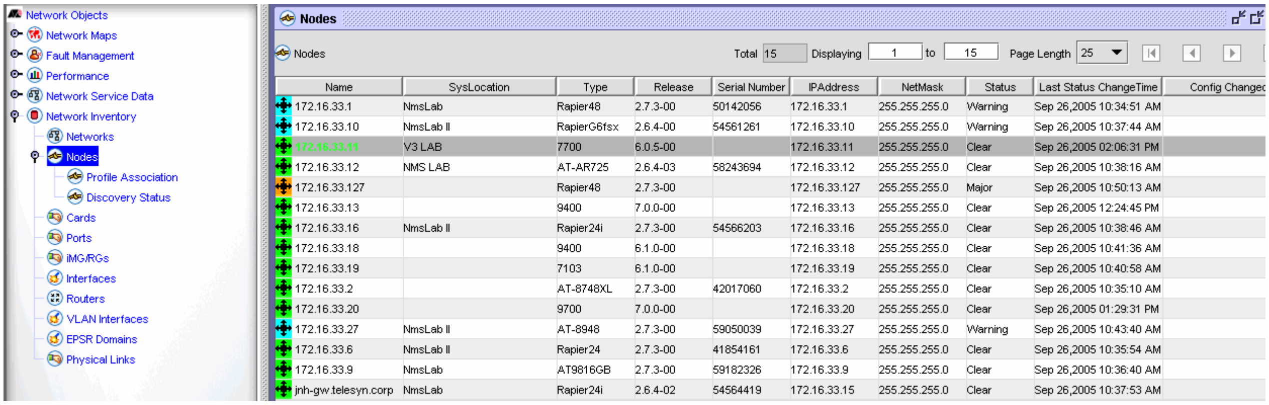
- *Managed Object Properties* - Displays the Managed Object Properties form for the selected object.
- *Delete Object and Traces* - Deletes the selected network object.
- *Stop Discovery* - Stops the discovery process in the selected network.
- *UnManage/Manage* - Marks the object as unmanaged if it is currently being managed, or as managed if the object is currently unmanaged. Managing an element means that you are setting the NMS to monitor its status. Unmanaging an element means that you are stopping the NMS from monitoring the element.

  Once a selected device is made managed (by selecting on the *Manage* menu item of either the table pop-up menu or the *Network* menu in the Panel-Specific Menu Bar), the icon displayed for the device will indicate the severity status of the device. The same icon will become gray in color when the selected device is made unmanaged by clicking the corresponding menu item. These menu items are also accessible from the object-specific menus.
- *Update Status* - Updates the status information for the selected object. If any changes have been made to the object (such as clearing alarms), clicking this will update the row.

5.2.2 Nodes Subview

The Nodes subview narrows the Network Inventory view to the nodes on the network. To access this view, click on the Nodes node under Network Inventory in the NMS Tree. An example is shown in the following figure.

Note: *It is possible to sort the Modes by Config Changed, so the user can see the latest nodes that have had their configurations changed and acknowledged by the Device Backup operation (for recurring backups).*



Name	SysLocation	Type	Release	Serial Number	IPAddress	NetMask	Status	Last Status ChangeTime	Config Changed
172.16.33.1	NmsLab	Rapier48	2.7.3-00	50142056	172.16.33.1	255.255.255.0	Warning	Sep 26,2005 10:34:51 AM	
172.16.33.10	NmsLab II	RapierG6fsx	2.6.4-00	54561261	172.16.33.10	255.255.255.0	Warning	Sep 26,2005 10:37:44 AM	
172.16.33.11	V3 LAB	7700	6.0.5-00		172.16.33.11	255.255.255.0	Clear	Sep 26,2005 02:06:31 PM	
172.16.33.12	NMS LAB	AT-AR725	2.6.4-03	58243694	172.16.33.12	255.255.255.0	Clear	Sep 26,2005 10:38:16 AM	
172.16.33.127		Rapier48	2.7.3-00		172.16.33.127	255.255.255.0	Major	Sep 26,2005 10:50:13 AM	
172.16.33.13		9400	7.0.0-00		172.16.33.13	255.255.255.0	Clear	Sep 26,2005 12:24:45 PM	
172.16.33.16	NmsLab II	Rapier24i	2.7.3-00	54566203	172.16.33.16	255.255.255.0	Clear	Sep 26,2005 10:38:46 AM	
172.16.33.18		9400	6.1.0-00		172.16.33.18	255.255.255.0	Clear	Sep 26,2005 10:41:36 AM	
172.16.33.19		7103	6.1.0-00		172.16.33.19	255.255.255.0	Clear	Sep 26,2005 10:40:58 AM	
172.16.33.2		AT-8748XL	2.7.3-00	42017060	172.16.33.2	255.255.255.0	Clear	Sep 26,2005 10:35:10 AM	
172.16.33.20		9700	7.0.0-00		172.16.33.20	255.255.255.0	Clear	Sep 26,2005 01:29:31 PM	
172.16.33.27	NmsLab II	AT-8948	2.7.3-00	59050039	172.16.33.27	255.255.255.0	Warning	Sep 26,2005 10:43:40 AM	
172.16.33.6	NmsLab II	Rapier24	2.7.3-00	41854161	172.16.33.6	255.255.255.0	Clear	Sep 26,2005 10:35:54 AM	
172.16.33.9	NmsLab	AT9816GB	2.7.3-00	59182326	172.16.33.9	255.255.255.0	Clear	Sep 26,2005 10:36:40 AM	
jnh-gw.telesyn.corp	NmsLab	Rapier24i	2.6.4-02	54564419	172.16.33.15	255.255.255.0	Clear	Sep 26,2005 10:37:53 AM	

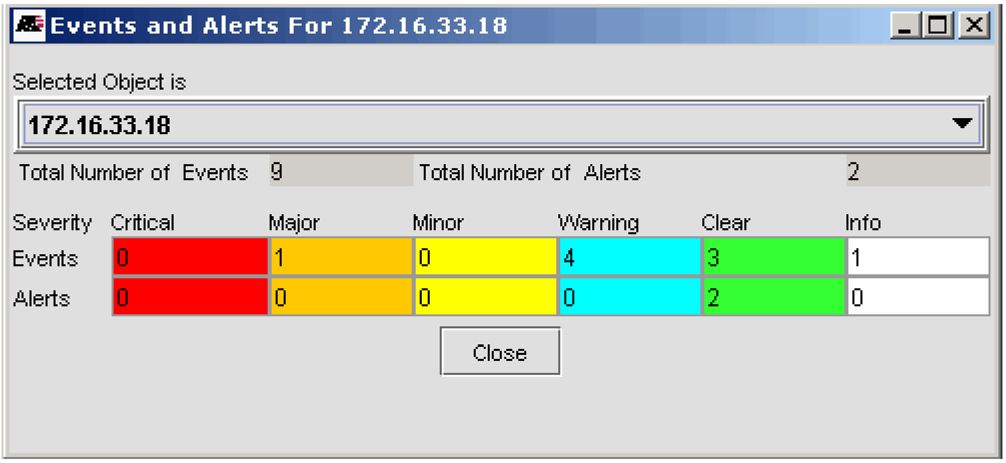
FIGURE 5-3 Example Nodes Subview

When the Nodes subview is displayed in the NMS Display Panel or when a node object is selected in the Network Inventory view, the *Operations* menu appears in the Panel-Specific Menu Bar. In the Nodes subview, this menu appears when a node is selected in the view.

Note: If multiple nodes are selected and the nodes are of different types (e.g. Rapier, 9400, etc.), the Object menu will appear instead of the Operations menu.

The items in the *Operations* menu include:

- *View Chassis* - Displays the current chassis view for the selected device.
- *View Device Log* - Displays the Device Log Viewer.
- *Provision* - Provides provisioning functions for the selected device.
- *Network Services* - Provides network link and VLAN functions for the selected device.
- *Alarms/Events* - Displays the alarms or events, or a summary of the alarms and events for the selected device. Selecting this and then choosing Alarms or Events will bring up the Alarms or Events view. Selecting *Summary* will bring up the Events and Alerts display, which gives a summary of the Events and Alerts. Refer to the following figure.



Events and Alerts For 172.16.33.18

Selected Object is

172.16.33.18

Total Number of Events 9 Total Number of Alerts 2

Severity	Critical	Major	Minor	Warning	Clear	Info
Events	0	1	0	4	3	1
Alerts	0	0	0	0	2	0

FIGURE 5-4 Summary Display for Events and Alarms (One Device)

- *Performance* - Brings up the Configured Collection window for the selected device.
- *View Config Comparison* - Brings up the Config Comparison Form. This is used for only non-i MAP devices, and must be text files.
- *Discover Attached iMGS/RGs* - If there are subtending iMGs/RGs, they are discovered. This is used in a variety of provisioning scenarios.
- *Display Switch FDB* - For swith (layer 2) devices, lists the Port, MAC, and VLAN association, as well as the Status.
- *Power over Ethernet Management*
- *Telnet To Device* - Opens a Telnet session to the selected device.
- *Browse Device* - Brings up the HTML browser for the device.
- *Rediscover Device* - Re-discovers the device immediately.
- *Managed Object Properties* - Displays the Managed Object Properties form for the selected device.
- *Delete Object and Traces* - Deletes the selected object.
- *UnManage/Manage* - Sets the device to unmanaged if it is currently managed, or managed if it is currently unmanaged.
- *Update Status* - Updates the event and alarm information on the selected device.

5.2.3 Profile Association

This subview shows which profiles are associated with which devices. If the attributes are not in synch, a * appears next to the Profile name and the profile should be reapplied.

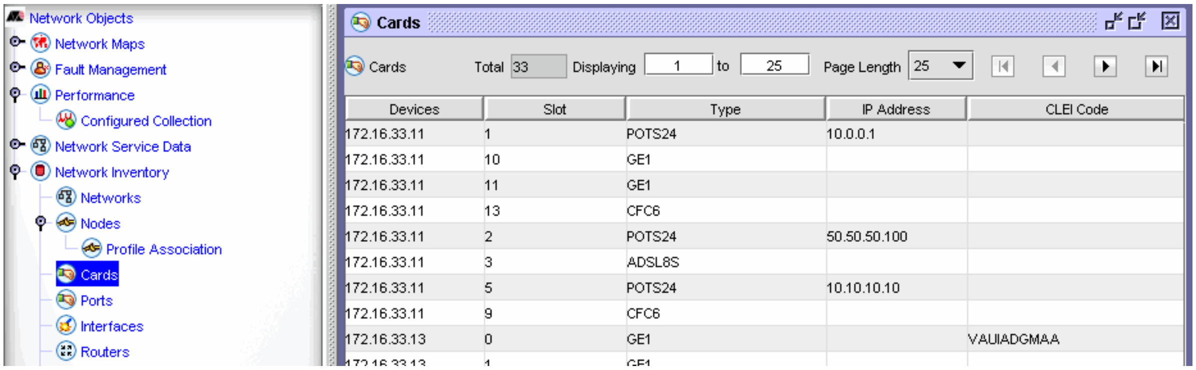
5.2.4 Discovery Status

This subview provides a quick way to see when a device was last discovered and whether the device passed or failed. It also gives the date of when the configuration of the device was last changed.

Note: This subview also includes the RG devices.

5.2.5 Customer Cards Subview

The Customer Card subview narrows the Network Inventory view to the customer cards. To access this view, click on the Cards node under Network Inventory in the NMS Tree. An example is shown in the following figure.



Cards Total 33 Displaying 1 to 25 Page Length 25

Devices	Slot	Type	IP Address	CLEI Code
172.16.33.11	1	POTS24	10.0.0.1	
172.16.33.11	10	GE1		
172.16.33.11	11	GE1		
172.16.33.11	13	CFC6		
172.16.33.11	2	POTS24	50.50.50.100	
172.16.33.11	3	ADSL8S		
172.16.33.11	5	POTS24	10.10.10.10	
172.16.33.11	9	CFC6		
172.16.33.13	0	GE1		VAUIADGMAA
172.16.33.13	1	GE1		

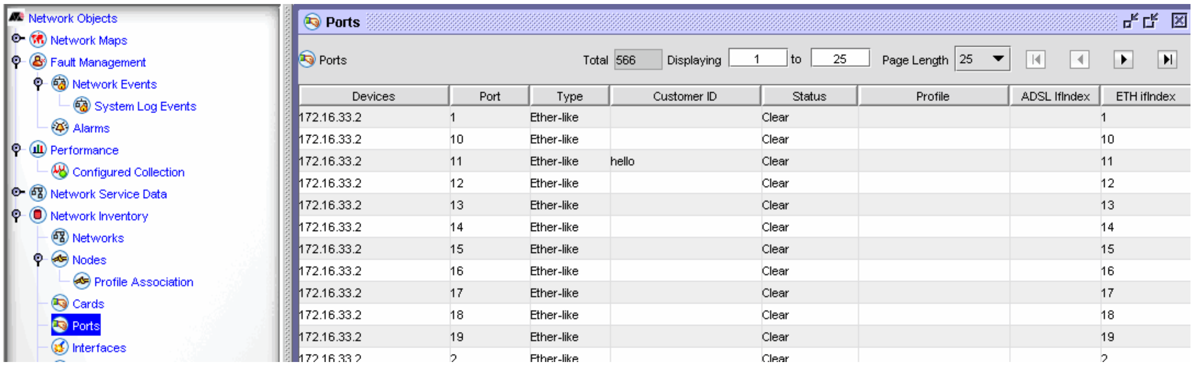
FIGURE 5-5 Example Customer Cards Subview

When the Customer Cards subview is displayed in the NMS Display Panel or when a customer port is selected in the Network Inventory view, the *Card* menu appears in the Panel-Specific Menu Bar, which is specific to customer ports. In the Customer Ports subview, this menu appears when you select a port. The items in the menu include:

- *View/Modify Details* - Displays the Port Management form for the selected port, which is used to manage (display and modify) the attributes of the port.
- *Remove Association with Profile* - Removes the association, so changing an attribute does not show the card as being Out-of-Profile.
- *Compare Card with Profile* - If the card has a Profile, compares the attributes and highlights what is not the same. (If the card has no Profile, there is the error message Profile not found.)
- *Audit CES Circuiits* - For CES cards, brings up the Diagnostic Audit screen
- *Alarms/Events* - Brings up the submenu to view associated alarms, events, or a summary.
- *Delete Object and Traces* - Deletes the selected card.

5.2.6 Customer Ports Subview

The Customer Ports subview narrows the Network Inventory view to the customer ports. To access this view, click on the Ports node under Network Inventory in the NMS Tree. An example is shown in the following figure.



Total 566 Displaying 1 to 25 Page Length 25

Devices	Port	Type	Customer ID	Status	Profile	ADSL IfIndex	ETH ifIndex
172.16.33.2	1	Ether-like		Clear			1
172.16.33.2	10	Ether-like		Clear			10
172.16.33.2	11	Ether-like	hello	Clear			11
172.16.33.2	12	Ether-like		Clear			12
172.16.33.2	13	Ether-like		Clear			13
172.16.33.2	14	Ether-like		Clear			14
172.16.33.2	15	Ether-like		Clear			15
172.16.33.2	16	Ether-like		Clear			16
172.16.33.2	17	Ether-like		Clear			17
172.16.33.2	18	Ether-like		Clear			18
172.16.33.2	19	Ether-like		Clear			19
172.16.33.2	2	Ether-like		Clear			2

FIGURE 5-6 Example Customer Ports Subview

When the Customer Ports subview is displayed in the NMS Display Panel or when a customer port is selected in the Network Inventory view, the *Port* menu appears in the Panel-Specific Menu Bar, which is specific to customer ports. In the Customer Ports subview, this menu appears when you select a port. The items in the menu include:

- *View/Modify Details* - Displays the Port Management form for the selected port, which is used to manage (display and modify) the attributes of the port.
- *Provision New Customer/Port* - Brings up the appropriate form to provision this port. This form can be the **Provision New Triple Play Customer Form** or the **Provision new DS1/E1 Port Form**.
- **De-provision Customer/Port** - If the port has already been provisioned, this form appears.

Note: In the EE version, the previous two items are not available.

- *Remove Association with Profile* - If a profile has been created and associated with the port, this option removes that association. Note that this does not affect the profile.
- *Compare Port with Profile* - Compares the attributes of the port with its profile. A window then appears that lists where attributes do not match (or the message No Differences).
- *Alarms/Events* - Brings up the submenu to view associated alarms, events, or a summary.
- *Delete Object and Traces* - Deletes the selected port.

The Port Management tool is used for the administration and maintenance of customer ports. The tool is accessed from the Customer Ports view by right-clicking a port in the view, and then selecting *View/Modify Details* from the pop-up menu. It can also be accessed by selecting *Tools->Customer Management->View/Modify Customer Ports* from the Panel-Specific Menu Bar.

The three main tabbed forms are:

- Triple Play Service Management
- DS1
- E1

Viewing the Triple Play Service Management Port form shows the attributes for the associated interfaces:

- Ether-like
- ADSL
- SHDSL
- POTS
- EPON
- ONU
- NTE8

- CES

These are explained in the following subsections.

Note: The Statistics tab and Log tag are common across these interfaces and show all statistics and logs for all ports in the Triple Play service.

5.2.6.1 Ether-Like Port Management

The display is a tabbed panel where each tab displays specific information on the Ethernet-like port. The tabs are as follows:

- **Status** - Displays general status
- **Ether-Like Configuration** - These have subtabs:
  - General - The main configuration attributes for the port
  - Port Thresholds - Displays the threshold settings for the RMON counters
  - Device Data Collection - Configures the data collection configuration (intervals and buckets)
  - IP Filters - Displays information on any IP filters that are applied to the selected port
- **Statistics** - Displays the results of the set-up that was done in the Configuration tab
  - RMON Stats - Allows enabling/disabling of performance and fault statistics
  - Graph Stats - Allows selecting and graphing of up to six statistics
- **Port Log** - Displays any log messages associated with the selected port

5.2.6.2 ADSL Port Management

The display is a tabbed panel where each tab displays specific information on the ADSL port. The tabs are as follows:

- **Status** - Displays general status
- **ADSL Configuration** - These have subtabs:
  - General - Displays general status and configuration information for the selected port.
  - VCs/VLANs - Correlates the port to Virtual Channels (VCs) and then the VC to one or more (up to four) VLANs.
  - PMON Thresholds - Allows thresholds to be set for the ATU-C and ATU-R statistics.
  - Device Data Coll. - Configures buckets that will collect statistics and the interval at which they are filled
  - IP Filters - Allows classifiers to be applied to the port.
- **Statistics** - These have subtabs:
  - PMON Stats - Collects traffic statistics over a specified time period (called the interval).
  - RMON Stats - Tracks packet flows and highlights errors as well as overflows of packets.
  - Graph Stats - Makes graphs both in real-time and for statistics that have been collected.
- **Port Log** - Displays any log messages associated with the selected port

5.2.6.3 SHDSL Port Management

The display is a tabbed panel where each tab displays specific information on the SHSDL port. The tabs are as follows:

- **Status** - Displays general status
- **SHDSL Configuration** - These have subtabs:
  - General - Displays general status and configuration information for the selected port
  - VCs/VLANs - Correlates the port to Virtual Channels (VCs) and then the VC to one or more VLANs. Note that in this release only one VLAN can be associated with the VC.

  - PMON Thresholds -
  - Device Data Collection - Configures buckets that will collect statistics and the interval at which they are filled
  - IP Filters - Allows classifiers to be applied to the port
- **Statistics**
  - PMON Stats - Collects traffic statistics over a specified time period (called the interval)
  - RMON Stats - Tracks packet flows and highlights errors as well as overflows of packets.
  - Graph Stats - Makes graphs both in real-time and for statistics that have been collected
- **Port Log** - Displays any log messages associated with the selected port

5.2.6.4 POTS Port Management

The display is a tabbed panel where each tab displays specific information on the POTS24 port. The tabs are as follows:

- **Status** - Displays general status
- **Voice Configuration**
  - POTS - The main attributes of the POTS port
- **Statistics**
  - POTS Stats - Lists the RTP statistics.
  - Graph Stats- Makes a graph of selected statistics and displays them with varying attributes
- **Diagnostics**
  - POTS - allows the user to run a set of diagnostics on the port interface
- **Port Log** - Lists all the port-related management logs that have been generated.

5.2.6.5 DS1/E1 Port Management

The display is a tabbed panel where each tab displays specific information on the DS1/E1 port. The tabs are as follows:

Note: The form is the same for dual endpoints, but the panels/fields are changed to accommodate two rather than one DS1/E1 port.

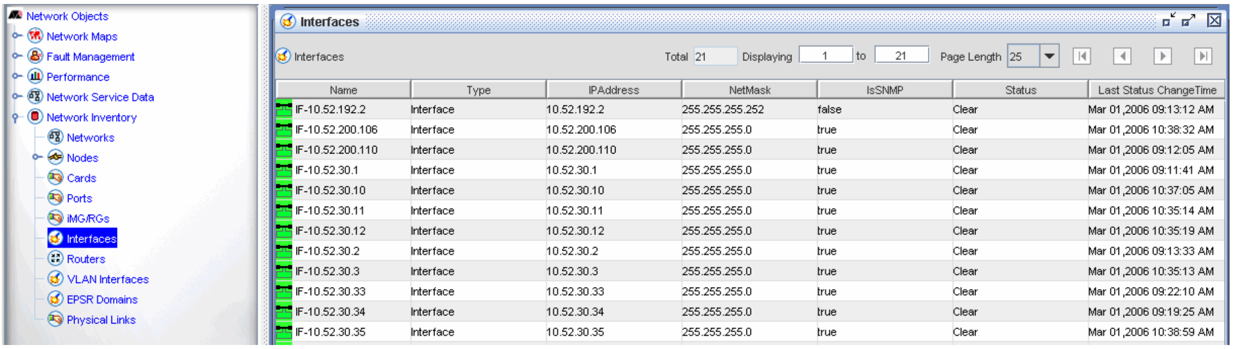
- **Status** - Displays general status
- **DS1/E1 Port -** Lists the status and main attributes of the port.
- **PSPAN** - Lists the attributes for the PSPAN. For dual endpoints, the initially selected port is what is on the left panel of the form.
- **PMON Statistics** - Enables for viewing the port and PSPAN statistics.
- **Stats Graph** - Makes a graph of selected statistics and displays them with varying attributes. For dual endpoints, the statistics are suffixed with an -A and -Z.
- **Port Thresholds** - Sets the DS1 and PSPAN thresholds that will activate a log and event.
- **Port Log** - Lists all the port-related management logs that have been generated

5.2.7 iMG/RGs Subview

This subview shows the iMGs/RGs and shows its main attributes (such as Customer ID) as well as profile association.

5.2.8 Interfaces Subview

The Interfaces subview narrows the Network Inventory view to the network interfaces. To access this view, click on the Interfaces node under Network Inventory in the NMS Tree. An example is shown in the following figure.



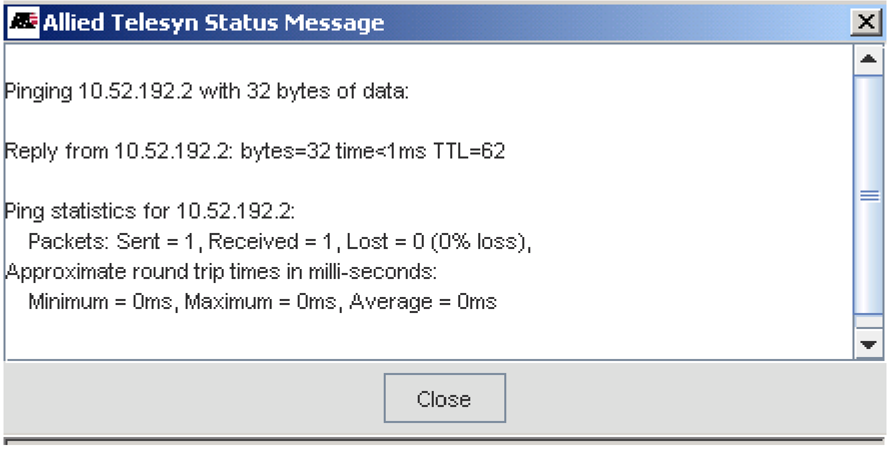
Interfaces Total 21 Displaying 1 to 21 Page Length 25

Name	Type	IPAddress	NetMask	IsSNMP	Status	Last Status ChangeTime
IF-10.52.192.2	Interface	10.52.192.2	255.255.255.252	false	Clear	Mar 01 ,2006 09:13:12 AM
IF-10.52.200.106	Interface	10.52.200.106	255.255.255.0	true	Clear	Mar 01 ,2006 10:38:32 AM
IF-10.52.200.110	Interface	10.52.200.110	255.255.255.0	true	Clear	Mar 01 ,2006 09:12:05 AM
IF-10.52.30.1	Interface	10.52.30.1	255.255.255.0	true	Clear	Mar 01 ,2006 09:11:41 AM
IF-10.52.30.10	Interface	10.52.30.10	255.255.255.0	true	Clear	Mar 01 ,2006 10:37:05 AM
IF-10.52.30.11	Interface	10.52.30.11	255.255.255.0	true	Clear	Mar 01 ,2006 10:35:14 AM
IF-10.52.30.12	Interface	10.52.30.12	255.255.255.0	true	Clear	Mar 01 ,2006 10:35:19 AM
IF-10.52.30.2	Interface	10.52.30.2	255.255.255.0	true	Clear	Mar 01 ,2006 09:13:33 AM
IF-10.52.30.3	Interface	10.52.30.3	255.255.255.0	true	Clear	Mar 01 ,2006 10:35:13 AM
IF-10.52.30.33	Interface	10.52.30.33	255.255.255.0	true	Clear	Mar 01 ,2006 09:22:10 AM
IF-10.52.30.34	Interface	10.52.30.34	255.255.255.0	true	Clear	Mar 01 ,2006 09:19:25 AM
IF-10.52.30.35	Interface	10.52.30.35	255.255.255.0	true	Clear	Mar 01 ,2006 10:38:59 AM

FIGURE 5-7 Example Interfaces Subview

When the Interfaces subview is displayed in the Display Panel or when a network interface object is selected in the Network Inventory view, the *Interface* menu appears in the Panel-Specific Menu Bar, which is specific to network interfaces. In the Interfaces subview, this menu appears when you select an interface in the view. This menu provides various functions in the interface. The items include:

- *InterfaceMonitor* - Provides a ping function, which allows you to ping the selected interface. Refer to the following figure. Selecting this item brings up the Status Message window, which contains the ping results. Refer to the following figure.



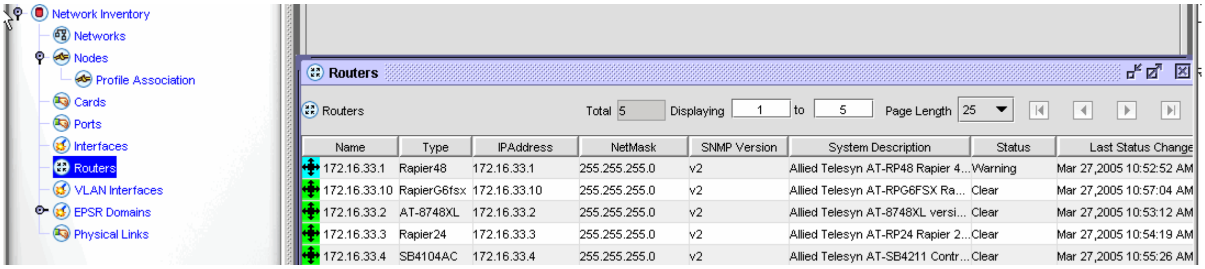
```
Pinging 10.52.192.2 with 32 bytes of data:

Reply from 10.52.192.2: bytes=32 time<1ms TTL=62

Ping statistics for 10.52.192.2:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

FIGURE 5-8 Ping Result Display

- *Managed Object Properties* - Displays the Managed Object Properties form for the selected interface.
- *Delete Object and Traces* - Deletes the selected interface.
- *UnManage/Manage* - Marks the selected interface as unmanaged if it currently is being managed, or as managed if it is currently unmanaged.
- *Update Status* - Updates the status information for the selected interface.

5.2.9 Routers Subview

The Routers subview narrows the Network Inventory view to the routers on the network. To access this view, click on the Routers node under Network Inventory in the NMS Tree. An example is shown in the following figure.



Routers Total 5 Displaying 1 to 5 Page Length 25

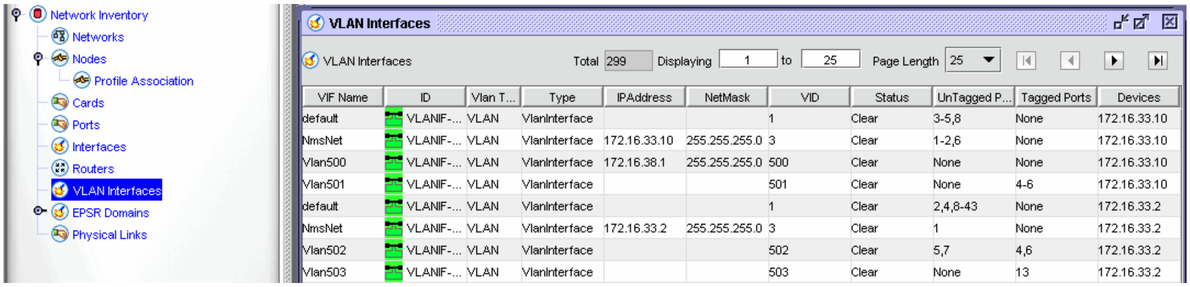
Name	Type	IPAddress	NetMask	SNMP Version	System Description	Status	Last Status Change
172.16.33.1	Rapier48	172.16.33.1	255.255.255.0	v2	Allied Telesyn AT-RP48 Rapier 4...	Warning	Mar 27,2005 10:52:52 AM
172.16.33.10	RapierG6fsx	172.16.33.10	255.255.255.0	v2	Allied Telesyn AT-RPG6FSX Ra...	Clear	Mar 27,2005 10:57:04 AM
172.16.33.2	AT-8748XL	172.16.33.2	255.255.255.0	v2	Allied Telesyn AT-8748XL versi...	Clear	Mar 27,2005 10:53:12 AM
172.16.33.3	Rapier24	172.16.33.3	255.255.255.0	v2	Allied Telesyn AT-RP24 Rapier 2...	Clear	Mar 27,2005 10:54:19 AM
172.16.33.4	SB4104AC	172.16.33.4	255.255.255.0	v2	Allied Telesyn AT-SB4211 Contr...	Clear	Mar 27,2005 10:55:26 AM

FIGURE 5-9 Example Routers Subview

When the Routers subview is displayed in the NMS Display Panel or when a router object is selected in the Network Inventory view, the *Operations* menu appears in the Panel-Specific Menu Bar. In the Routers subview, this menu appears when you select a router in the view. This is the same *Operations* menu that appears in the Nodes subview. Refer to "Nodes Subview" on page 76.

5.2.10 VLAN Interfaces Subview

The VLAN Interfaces subview narrows the Network Inventory view to the VLAN interfaces on the network. To access this view, click on the VLAN Interfaces node under Network Inventory in the NMS Tree. An example is shown in the following figure.



VLAN Interfaces Total 299 Displaying 1 to 25 Page Length 25

VIF Name	ID	Vlan T...	Type	IPAddress	NetMask	VID	Status	UnTagged P...	Tagged Ports	Devices
default	VLANIF-...	VLAN	VlanInterface			1	Clear	3-5,8	None	172.16.33.10
NmsNet	VLANIF-...	VLAN	VlanInterface	172.16.33.10	255.255.255.0	3	Clear	1-2,6	None	172.16.33.10
Vlan500	VLANIF-...	VLAN	VlanInterface	172.16.38.1	255.255.255.0	500	Clear	None	None	172.16.33.10
Vlan501	VLANIF-...	VLAN	VlanInterface			501	Clear	None	4-6	172.16.33.10
default	VLANIF-...	VLAN	VlanInterface			1	Clear	2,4,8-43	None	172.16.33.2
NmsNet	VLANIF-...	VLAN	VlanInterface	172.16.33.2	255.255.255.0	3	Clear	1	None	172.16.33.2
Vlan502	VLANIF-...	VLAN	VlanInterface			502	Clear	5,7	4,6	172.16.33.2
Vlan503	VLANIF-...	VLAN	VlanInterface			503	Clear	None	13	172.16.33.2

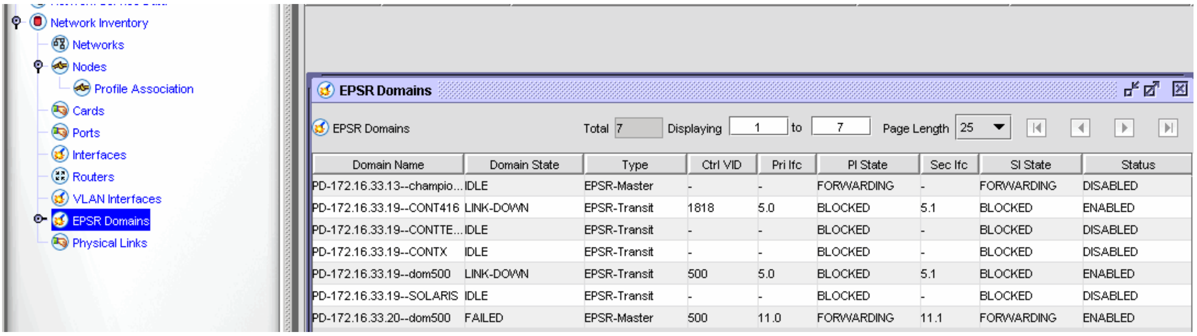
FIGURE 5-10 Example VLAN Interfaces Subview

When the VLAN Interfaces subview is displayed in the NMS Display Panel or when a VLAN interface is selected in the Network Inventory view, the *VLAN Interfaces* menu appears in the Panel-Specific Menu Bar, which is specific to VLAN interfaces. In the VLAN Interfaces subview, the menu appears when an interface is selected in the view. This menu provides various functions on VLAN interfaces. The menu items include:

- *Configure VLAN Interface* - Provides functions for configuring the selected VLAN interface.
- *Extend Vlan* - Provides functions for extending a VLAN.
- *Alarms/Events* - Provides alarm and event information for the selected VLAN interface.
- *Managed Object Properties* - Displays the Managed Object Properties form for the selected VLAN interface.
- *Delete Object and Traces* - Deletes the selected VLAN interface.
- *UnManage/Manage* - Marks the selected VLAN interface as unmanaged if it currently is being managed, or as managed if it is currently unmanaged.
- *Update Status* - Updates the status information on the selected VLAN interface.

5.2.11 EPSR Domains Subview

The EPSR Domains Subview is a way to see in list format all of the domains that have been defined and the devices/control VLANs that are part of that domain. Refer to the following figure.



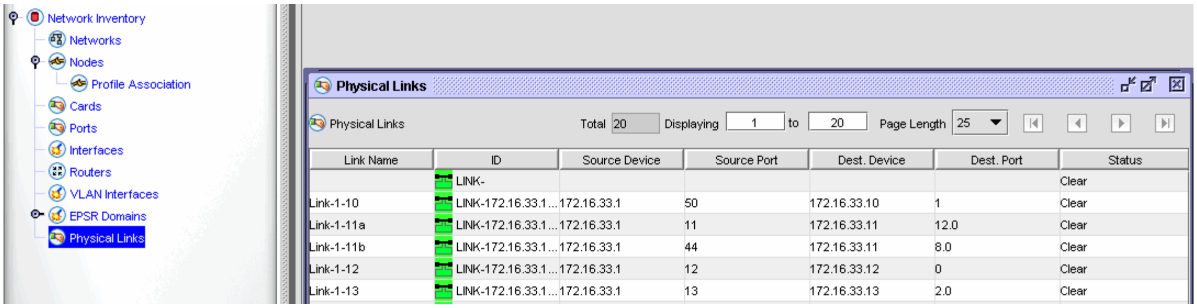
EPSR Domains Total 7 Displaying 1 to 7 Page Length 25

Domain Name	Domain State	Type	Ctrl VID	Pri Ifc	PI State	Sec Ifc	SI State	Status
PD-172.16.33.13--champio...	IDLE	EPSR-Master	-	-	FORWARDING	-	FORWARDING	DISABLED
PD-172.16.33.19--CONT416	LINK-DOWN	EPSR-Transit	1818	5.0	BLOCKED	5.1	BLOCKED	ENABLED
PD-172.16.33.19--CONTTE...	IDLE	EPSR-Transit	-	-	BLOCKED	-	BLOCKED	DISABLED
PD-172.16.33.19--CONTX	IDLE	EPSR-Transit	-	-	BLOCKED	-	BLOCKED	DISABLED
PD-172.16.33.19--dom500	LINK-DOWN	EPSR-Transit	500	5.0	BLOCKED	5.1	BLOCKED	ENABLED
PD-172.16.33.19--SOLARIS	IDLE	EPSR-Transit	-	-	BLOCKED	-	BLOCKED	DISABLED
PD-172.16.33.20--dom500	FAILED	EPSR-Master	500	11.0	FORWARDING	11.1	FORWARDING	ENABLED

FIGURE 5-11 EPSR Domains Subview

5.2.12 Physical Links Subview

The Physical Links subview narrows the Network Inventory view to the physical links on the network. To access this view, click on the Physical Links node under Network Inventory in the NMS Tree. An example is shown in the following figure.



Physical Links Total 20 Displaying 1 to 20 Page Length 25

Link Name	ID	Source Device	Source Port	Dest. Device	Dest. Port	Status
	LINK-					Clear
Link-1-10	LINK-172.16.33.1...	172.16.33.1	50	172.16.33.10	1	Clear
Link-1-11a	LINK-172.16.33.1...	172.16.33.1	11	172.16.33.11	12.0	Clear
Link-1-11b	LINK-172.16.33.1...	172.16.33.1	44	172.16.33.11	8.0	Clear
Link-1-12	LINK-172.16.33.1...	172.16.33.1	12	172.16.33.12	0	Clear
Link-1-13	LINK-172.16.33.1...	172.16.33.1	13	172.16.33.13	2.0	Clear

FIGURE 5-12 Example Physical Links Subview

When the Physical Links subview is displayed in the NMS Display Panel or when a physical link object is selected in the Network Inventory view, the *Link* menu appears in the Panel-Specific Menu Bar, which is specific to physical links. In the Physical Links subview, the menu appears when a link is selected in the view. This menu provides various functions on physical links. The menu items include:

- *Link Operations* - This brings up the Layer 2 form that allows the user to add or delete physical links.
- *Managed Object Properties* - Displays the Managed Object Properties form for the selected link.
- *Alarms/Events* - Provides alarm and event information for the selected link.
- *UnManage/Manage* - Marks the selected link as unmanaged if it currently is being managed, or as managed if it is currently unmanaged
- *Update Status* - Updates the status information on the selected link.

5.3 Creating Custom Views

Refer to Networks a list of properties that are commonly used to create meaningful custom views.

5.4 Adding a Node / Network without Discovery Configurator

The user can add networks and nodes in the Network Inventory screen as Managed Objects (not modifying the seed.file) and this will take effect immediately. The menu choice:

- *Network Inventory / Edit -> Add Network*

- *Network Inventory / Edit -> Add Node*

brings up the dialog to add a network or node.

5.5 Adding and Refreshing a Node

Select *Edit -> Add Node* from the Panel-Specific Menu Bar to add a new node to the existing object list in the Network Inventory panel.

6. Using the Fault Management View

Views are used in the AlliedView NMS to display information related to a specific aspect of network management, such as network events. The Fault Management view is a default view that displays information related to events, system logs, and alarms. In addition to the Fault Management view are two other default views: Performance and Network Inventory. These views display additional information on the network and are described later in this document. This section focuses on the Fault Management view and how it is used.

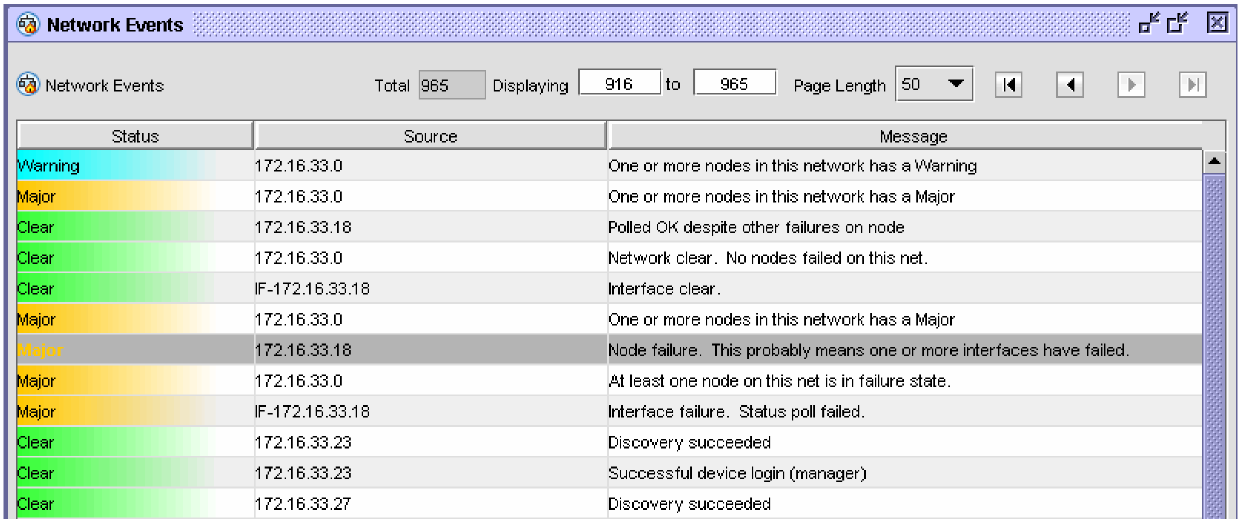
Network Events are entities that represent the various happenings in the network devices. Events can convey general information or the current status of the devices in a network. Working with the NMS, the user can know the history of a device by browsing through the Event Viewer in the client. The Event Viewer provides a wide range of features to the user in extracting the required information from the Network Events.

System logs are indications from individual devices that some change has occurred on the device. It may be a minor change in which case the log merely provides information, or it may be a significant change that requires attention, such as an alarm or failure. The System Log Events viewer, which is a subview of the Network Events view, provides a wide range of features to the user in extracting the required information from the system logs.

Alarms are generated when a failure or fault is detected in the network devices. The generated Alarms are displayed in the Alarm Viewer. The Alarm list containing alarms of various severity levels, such as critical, major, minor, clear, etc., can be viewed in the Alarm Viewer. The Alarm Viewer provides a wide range of features to the user in extracting the necessary information from the Alarms and viewing them in a specific way.

6.1 The Network Event View

This Event Viewer gets displayed on selecting the Network Events Panel under Fault Management of the NMS Tree as shown in the following figure.



Network Events

Total 965 Displaying 916 to 965 Page Length 50

Status	Source	Message
Warning	172.16.33.0	One or more nodes in this network has a Warning
Major	172.16.33.0	One or more nodes in this network has a Major
Clear	172.16.33.18	Polled OK despite other failures on node
Clear	172.16.33.0	Network clear. No nodes failed on this net.
Clear	IF-172.16.33.18	Interface clear.
Major	172.16.33.0	One or more nodes in this network has a Major
Major	172.16.33.18	Node failure. This probably means one or more interfaces have failed.
Major	172.16.33.0	At least one node on this net is in failure state.
Major	IF-172.16.33.18	Interface failure. Status poll failed.
Clear	172.16.33.23	Discovery succeeded
Clear	172.16.33.23	Successful device login (manager)
Clear	172.16.33.27	Discovery succeeded

FIGURE 6-1 Network Events Main Panel

As shown in Figure 6-1, the Network Events view presents information on all events that have occurred on the network.

Note: *The Node clear. No failures on this node event indicates the node was successfully polled and that the results show a previous failure on the node has cleared. When this event occurs, if no other alarm conditions exist on the node, the alarm severity for the node will change to green. However, if another alarm exists on the node, such as a Threshold Crossing Alarm (TCA), the alarm severity of the Node clear. No failures on this node event and the node will reflect the severity of the persisting alarm even though the event indicates no failures on the node. Please keep in mind that the Node clear. No failures on this node event means that all failures have been cleared on the node and not that all alarms have been cleared.*

6.1.1 Panel-Specific Menus for Views

As with Network Maps, the Panel-Specific Menu Bar is available for each view. Some of the menus are common to all views, while others are specific to an individual view. The relevant menus appear when a view is displayed in the NMS Display Panel.

6.1.1.1 Panel-Specific Menus Common to all Views

The panel-specific menus that are common to all views include:

- File
- Custom Views
- Tools
- Window
- Help

The *File*, *Tools*, *Window*, and *Help* menus are the same menus that appear for Network Maps. These menus are described in "Panel-Specific Menu Bar" on page 43. Although the *Custom Views* menu also appears for Network Maps, the items in this menu are different for views. For views, the items in the *Custom Views* menu include:

Add Custom View - Adds a custom view to the NMS Tree (custom views are described later in this document)

Remove Custom View - Removes a view from the NMS Tree

Modify Custom View - Modifies the filtering criteria for a view

Save Custom View State - Preserves the state of the current view displayed in the NMS Display Panel

Rename Custom View - Renames a view

6.1.1.2 Panel-Specific Menus for the Network Events View

When the Network Events view is displayed in the NMS Display Panel, the following menu items appear in the panel-specific menu that are specific to the Network Events view:

- *Edit* - Provides editing functions for the view. Items include:
  - *Configure* - Provides configuration functions for trap and event parsers, and for event filters.
  - *Search* - Provides a search function for the view (refer to "Searching in a View" on page 90).
  - *Export Table Data* - Provides an export function for all of the view data. The data may be exported to a file (in delimited tabular form) or to a Web browser. The data may also be filtered.
  - *Export Selected Rows* - Provides an export function for selected rows in the view data.
  - *Schedule Event Export* - The Events in the View can be exported to a file now or at a later time. There is a separate subsection ("Schedule Event Export" on page 88) to explain this feature.
- *View* - Provides additional display functions for the view. Items include:
  - *Event Details* - Brings up the Event Details Form, where attribute values can be seen.
  - *Source Details* - Brings up the Details Form, except as follows:

    - For the VLAN IF, the Chassis View appears.

  - For the iMG/RG, the Triple Play Service Management Form appears
  - For a port, brings up the Port Menagement Form

  - *Alarms* - Provides alarm information specific to the selected event.

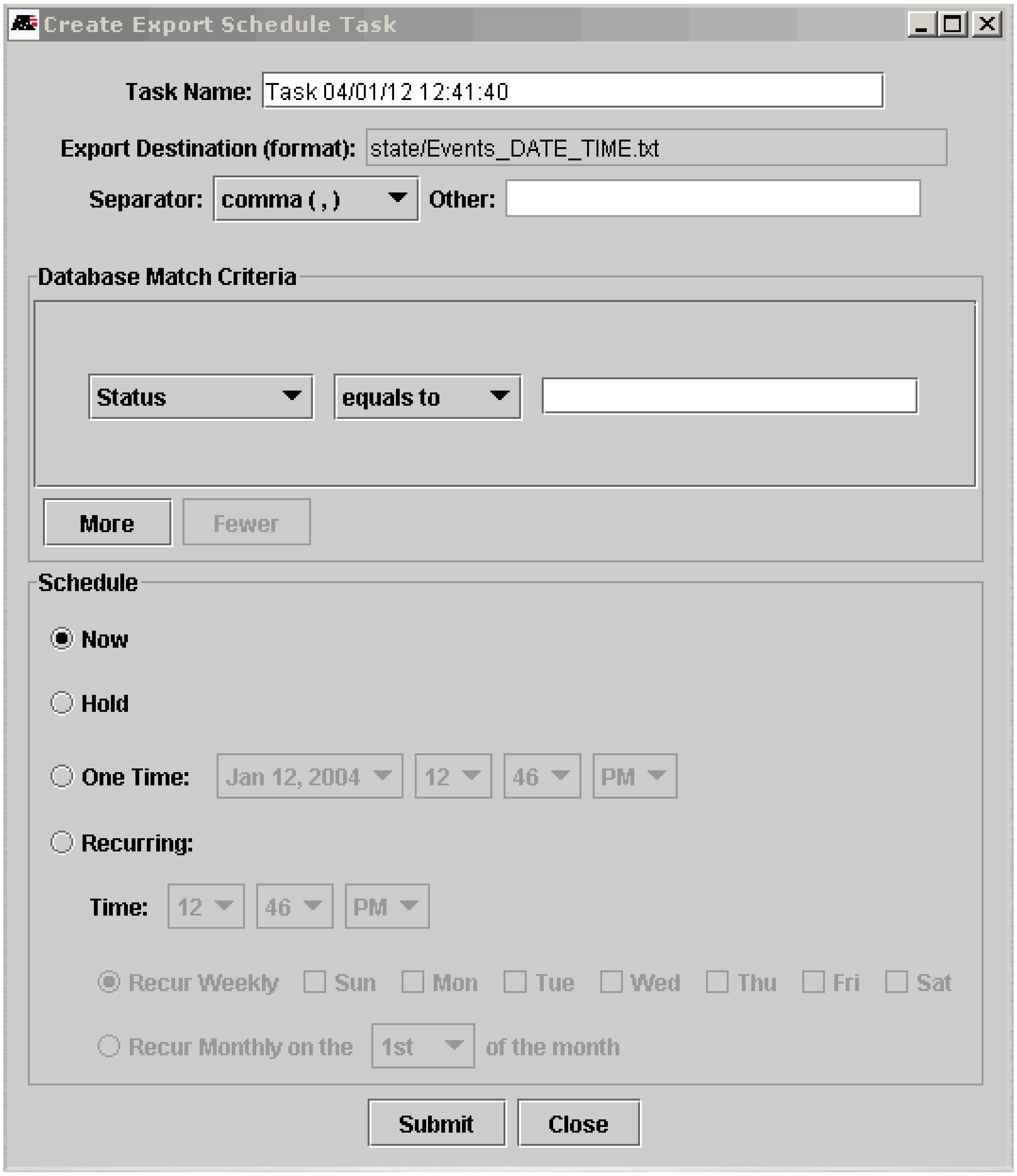
Note: Selecting this option will take you to the Alarms view.

  - *Refresh* - Refreshes the view information.

- *Actions* -
  - *Save To File* option, which saves the event information to a file.
  - *Export Events* -

6.1.1.3 Schedule Event Export

The menu item *Schedule Event Export* exports the event view to a file either now or a later time. Figure 6-2 shows the form that is displayed.



Create Export Schedule Task

Task Name: Task 04/01/12 12:41:40

Export Destination (format): state/Events_DATE_TIME.txt

Separator: comma (,) Other:

Database Match Criteria

Status equals to

Schedule

● Now

○ Hold

○ One Time: Jan 12, 2004 12 46 PM

○ Recurring:

Time: 12 46 PM

● Recur Weekly □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

○ Recur Monthly on the 1st of the month

FIGURE 6-2 Export Scheduler Task Window

This form is similar to other scheduling forms. Note the following:

- The words DATE and TIME in the Export Destination will be replaced by the date and time on the server when the schedule is executed and the names of files generated will have the actual date and time.
- Separator fields work the same way as they do in on-demand table data export and the selected separator will be used when the data is exported to text files.
- Match criteria fields (options) available on the screen are very similar to those in on-demand Events/Alerts Table Data Export.
- One new option in match criteria used instead of dates allows the user to select number of previous days within a range to be included in each of the scheduled export. The criteria is **Days/Range** and **within**.

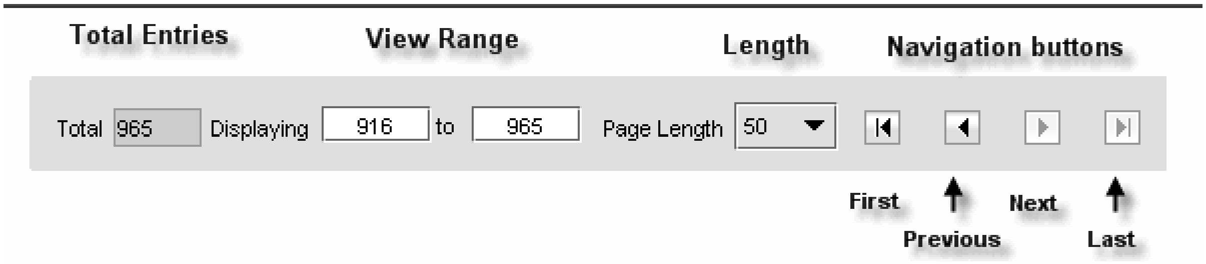
For example, the user may set a schedule to export of all critical events every day by selecting Recurring radio button and every day of the week checkboxes and set the Days/Range option to 1 to export daily data every day. For every week by the user would select one day in the Recurring schedule and set the Days/Range to 7 to export data for the past seven days once every week.

- The output files generated by each export are very similar to those generated by on-demand Events/Alerts Table Data Export. In the scheduled export there will be a new file every time the schedule is executed.

All schedule fields are the same as used in other schedule related operations such as NMS backup.

6.1.2 Navigating in a View

By using the Navigation Panel, the user can help isolate specific items in a view. Refer to the following figure.



Total 965 Displaying 916 to 965 Page Length 50

FIGURE 6-3 Navigation Panel

The Navigation Panel button functions are as follows:

- First – View the first page of the items
- Previous – View the previously viewed frame
- Next – View the next frame of items
- Last – View the last frame of items

The range of items to display is controlled by the View Range fields. You can also use the drop-down list to use the default ranges available.

You can sort the items based on the column type by clicking on the column. There are two types of sorting:

- Server – By clicking on the column, you sort the complete data. Clicking on the column again will toggle the ascending to descending. The sort indicators for server-side sorting for ascending and descending are ▼ and ▲, respectively
- Client – By pressing and holding the Ctrl key, and then clicking the column, you sort the client-side data. The sort indicator for client side sorting for ascending and descending are ▼ and ▲, respectively.

You can combine both in one column by performing both types of sorts. You can also reorder the columns by dragging a column header to the right or left.

Note: *When starting the client and opening the Network Events or Alarms panel for the first time, you will see the last page with the most recent events or alarms shown. Click the Date column twice, then click the First Page button, so that the most recent events or alarms appear on the first page in descending order (most recent event or alarm first).*

Note: *Sorting on IP Addresses results in lexical order, not numeric.*

6.1.2.1 Searching in a View

To search for specific items in a view, select *Edit -> Search* from the Panel-Specific Menu Bar, or click the Search button (🔍) in the Toolbar. This will display the search window shown in the figure, which will allow you to specify the search criteria.

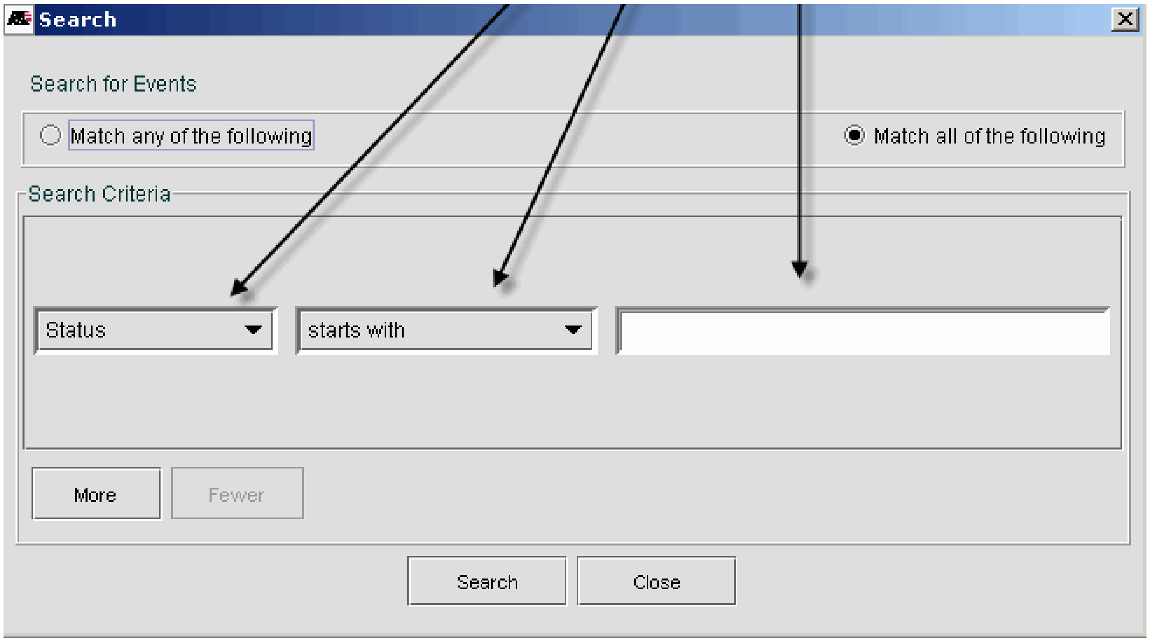


FIGURE 6-4 View Search Window

You can choose whether all the criteria or any of the criteria should match by clicking the **Match any of the following** or the **Match all of the following** radio button.

Each criteria is defined as the column name, a search pattern qualifier, and the search pattern. The column name can be selected from a drop-down list of the column names displayed in the current view. The search pattern qualifier can be selected from a list of the following:

- starts with
- doesn’t start with
- ends with
- doesn’t end with
- contains
- doesn’t contain
- equals
- not equals

The search pattern is the string to be matched in the search and is simply typed into the text box. To add additional criteria, click **More**. To begin the search, click **Search**.

When **Search** is clicked, the entries matching the search criteria will be displayed in the view, and the **Show All** button will appear to the right of the navigation buttons. (If no entries match the criteria, the view display will be blank.) To restore all of the entries in the view, click the **Show All** button.

Note: Searching on Date will result in incorrect match on current date.

The following behavior may be observed when searching on the Message column in Syslog Events:

- using the search pattern qualifier “starts with” or “ends with” takes a while to complete
- using the search pattern qualifier “equals” yields an empty result set
- using the search pattern qualifiers “doesn't start with”, “doesn't end with”, and “not equals” returns all messages including those that do not meet the criteria.

6.2 Creating Custom Views for Events

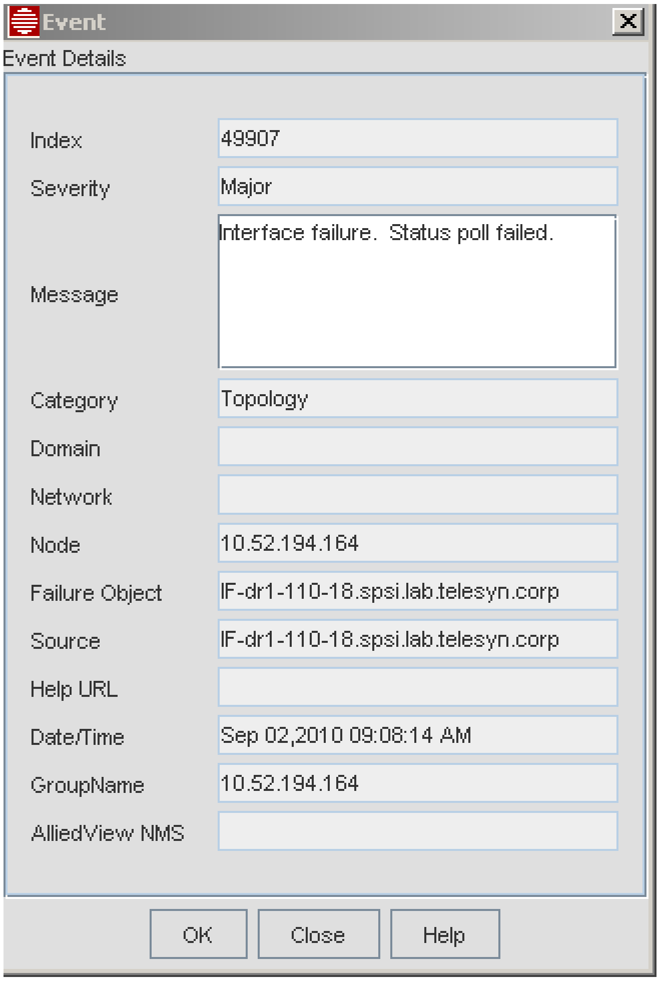
Refer to "Events" on page 1077 for a list of properties that are commonly used to create meaningful custom views.

6.3 Event View Tasks

6.3.1 Specify Event Details

Event Details gives detailed information about the properties of the event that is selected from the displayed Event viewer. The properties are displayed in the Details form in which you can view properties such as Severity, Message, Category etc.

By double-clicking any part of an event displayed in the Event Viewer, you can view the event property details. You can also select *View->Details* from the Panel-Specific Menu Bar to retrieve the property details after selecting the event. (The selected event will turn dark gray.) This brings up the Event Details form showing the common criteria, as shown in the following figure.



Index	49907
Severity	Major
Message	Interface failure. Status poll failed.
Category	Topology
Domain	
Network	
Node	10.52.194.164
Failure Object	IF-dr1-110-18.spsi.lab.telesyn.corp
Source	IF-dr1-110-18.spsi.lab.telesyn.corp
Help URL	
Date/Time	Sep 02,2010 09:08:14 AM
GroupName	10.52.194.164
AlliedView NMS	

FIGURE 6-5 Event Details Form

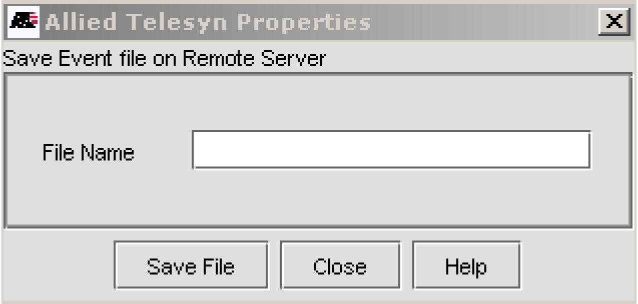
The following table lists the properties and their values.

TABLE 6-1 Event Detail Properties

Property	Description for Event Detail Properties
Index	A unique index number to every generated event.
Severity (Class)	The severity of the event to be filtered can be assigned here using the combo box. Multiple severity can also be assigned by separating them using comma.
Message	A property in the event object which stores any important additional information of the event. If you want to view the event with a particular message, then you may fill the message in this field, which will display the events with the corresponding message.
Category	The text that appears in the Category column if it is displayed.
Domain	Any domain-specific information based on physical location, functional categorization, or logical categorization of the source of the event.
Network	Information about the network to which the source of the event belongs is specified here.
Node	Any additional information about the source, or the source itself, of the event.
Failure Object	Information about the specific entity within the source of the event, which is primarily responsible for the occurrence of this alarm. The name of the failure object to be filtered can be given in this field.
Source	Information about the source of the alarm. The source based on which alarms are to be filtered can be given in this field.
Help URL	The URL of the help document related to the event, which is reached through the Help button at the bottom of the event details sheet.
Date/Time	An date/time after which events that occur are displayed in the custom view. In other words, events that occur after this date/time are displayed.
AlliedView NMS	The name of the AlliedView NMS.

6.3.2 Saving Events to a File

The event information displayed in a Network Events map can be saved to a file by selecting *Actions->Save To File* from the Panel-Specific Menu Bar or by clicking the **Save** icon (🖫) in the Toolbar. This will display the **Save Event file on Remote Server** window shown in the following figure.

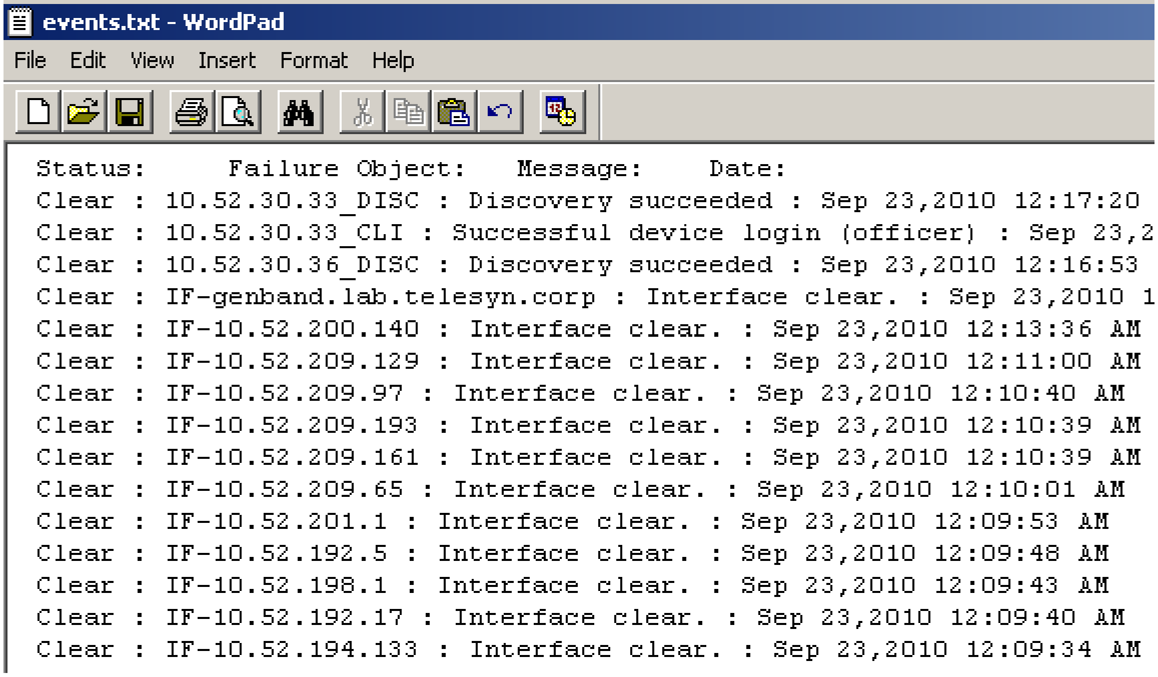

Allied Telesyn Properties

Save Event file on Remote Server

File Name

FIGURE 6-6 Save Event file on Remote Server Window

To save the information, type a file name in the File Name field, and then click the **Save File** button. A confirmation dialog box will appear indicating that the file was saved. You will find the file in directory `<Web NMS Home>/state`. The file will be an ASCII file that contains the event information in a colon-separated (:) list as shown in the following figure. You can open and view the file using any ASCII file editor, such as Notepad or vi.



```
Status:     Failure Object:   Message:    Date:
Clear : 10.52.30.33_DISC : Discovery succeeded : Sep 23,2010 12:17:20
Clear : 10.52.30.33_CLI : Successful device login (officer) : Sep 23,2
Clear : 10.52.30.36_DISC : Discovery succeeded : Sep 23,2010 12:16:53
Clear : IF-genband.lab.telesyn.corp : Interface clear. : Sep 23,2010 1
Clear : IF-10.52.200.140 : Interface clear. : Sep 23,2010 12:13:36 AM
Clear : IF-10.52.209.129 : Interface clear. : Sep 23,2010 12:11:00 AM
Clear : IF-10.52.209.97 : Interface clear. : Sep 23,2010 12:10:40 AM
Clear : IF-10.52.209.193 : Interface clear. : Sep 23,2010 12:10:39 AM
Clear : IF-10.52.209.161 : Interface clear. : Sep 23,2010 12:10:39 AM
Clear : IF-10.52.209.65 : Interface clear. : Sep 23,2010 12:10:01 AM
Clear : IF-10.52.201.1 : Interface clear. : Sep 23,2010 12:09:53 AM
Clear : IF-10.52.192.5 : Interface clear. : Sep 23,2010 12:09:48 AM
Clear : IF-10.52.198.1 : Interface clear. : Sep 23,2010 12:09:43 AM
Clear : IF-10.52.192.17 : Interface clear. : Sep 23,2010 12:09:40 AM
Clear : IF-10.52.194.133 : Interface clear. : Sep 23,2010 12:09:34 AM
```

FIGURE 6-7 Sample Event File

When saving these files, the AlliedView NMS sets as the default directory the <NMS Home>/state directory, so the file as entered in Figure 6-6 would be stored as:

<NMS Home>/state/NetEvents-AUG2003

If the user wishes to store the file in another directory, the path included must be relative to the default path. For example, if the user wishes to save the file in the <NMS Home>/conf directory, the user would enter

../conf/NetEvents-AUG2003

This will be shown in the status message when the file is successfully saved.

6.3.3 Configuring Trap Parsers

Configuring a trap parser is done to create and refine the information received from a trap (a specific unsolicited report by a device).

Configuring trap parsers can be done by using the information in the MIB to set the match criteria or by defining the configuration and saving it to a file.

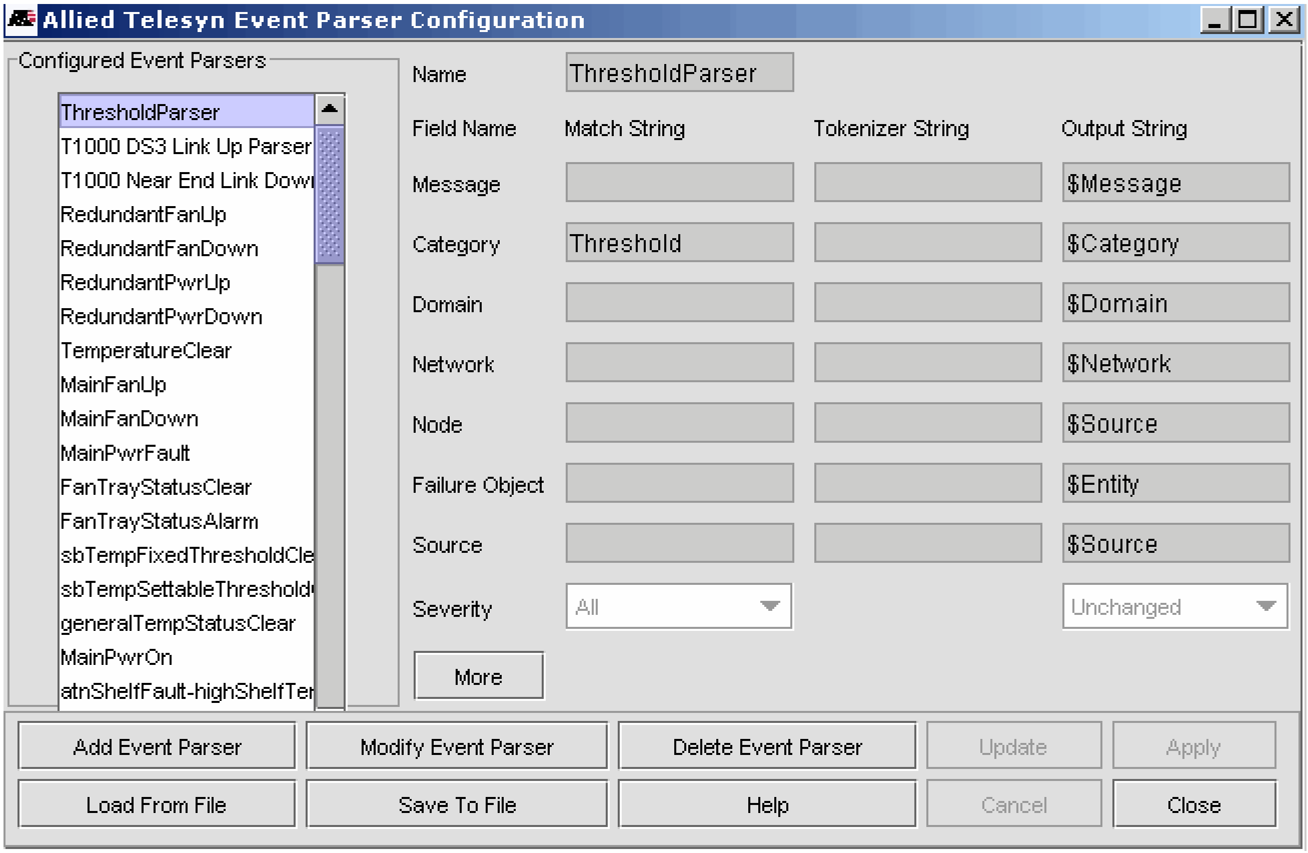
To configure a trap parser, select *Edit -> Configure > Trap Parsers* from the Panel-Specific Menu Bar for Network Events.

6.3.4 Configuring Event Parsers

When an event arrives into Web NMS, the event parsers list is checked to see whether the incoming event satisfies the match criteria of the event parser. If the event parser matches, the event is passed through the corresponding event parser. The outgoing event from the parser is then matched with the remaining set of parsers (if any, in sequence). If there are any matches, the event will be passed through those parsers. This process will continue until there are no parsers left to be scanned.

Configuring Event Parsers can be done by defining the Event Parser or the information or defining the configuration and saving it to a file.

To configure an event parser, select *Edit -> Configure > Event Parsers* from the Panel-Specific Menu Bar for Network Events. The Event Parser Configuration form will appear as shown in the following figure.



Allied Telesyn Event Parser Configuration

Configured Event Parsers

- ThresholdParser
- T1000 DS3 Link Up Parser
- T1000 Near End Link Dowi
- RedundantFanUp
- RedundantFanDown
- RedundantPwrUp
- RedundantPwrDown
- TemperatureClear
- MainFanUp
- MainFanDown
- MainPwrFault
- FanTrayStatusClear
- FanTrayStatusAlarm
- sbTempFixedThresholdCle
- sbTempSettableThreshold
- generalTempStatusClear
- MainPwrOn
- atnShelfFault-highShelfTe

Name: ThresholdParser

Field Name	Match String	Tokenizer String	Output String
Message			$Message
Category	Threshold		$Category
Domain			$Domain
Network			$Network
Node			$Source
Failure Object			$Entity
Source			$Source
Severity	All		Unchanged

FIGURE 6-8 Event Parser Configuration Form - File

In the Configured Event Parsers list on the Event Parser Configuration form, the user can view the list of currently configured event parsers. Clicking any of them will the display the corresponding details in the form. By default, the event parsers that are saved in the file **event.parsers** under <Web NMS Home>/conf directory will be loaded automatically when the server is started afresh. (cold start i.e., server is started after re initializing) and displayed in the list.

6.3.5 Configuring Event Filters

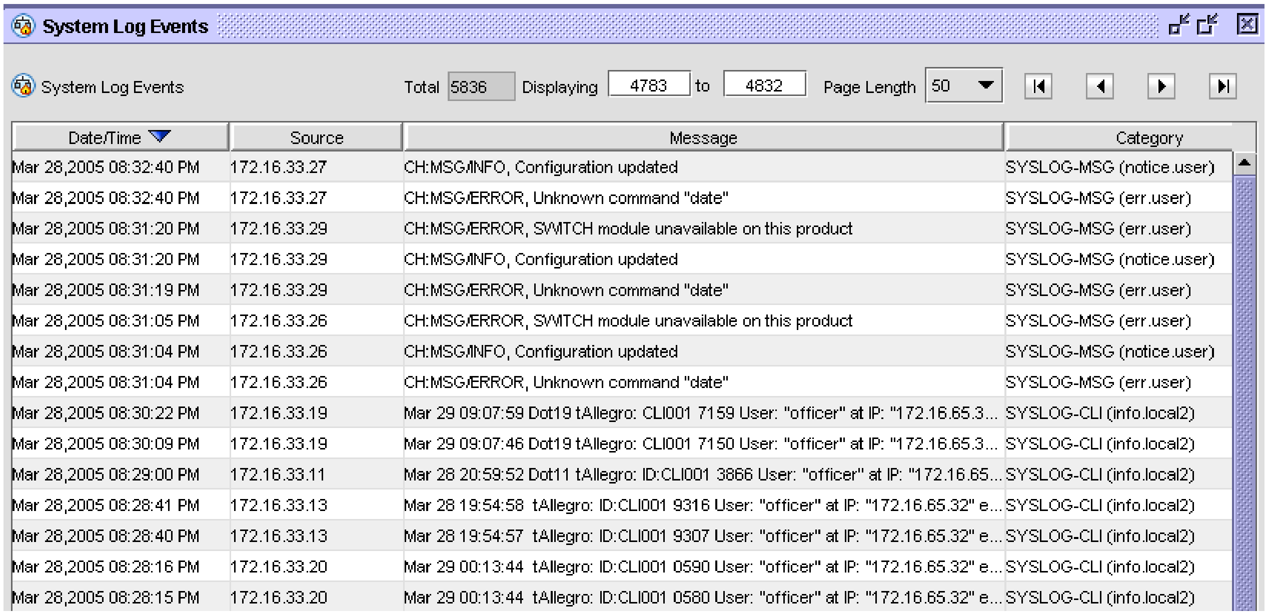
Event Filters provide a way of setting matching criteria to filter events and then configuring an action (such as an email) for those events. To configure an event filter, select *Edit -> Configure > Event Filters* from the Panel-Specific Menu Bar for Network Events.

6.3.6 Viewing Related Alarms

To view the related alarms for a particular event, click anywhere on the event row and select *View -> Alarms* from the Panel-Specific Menu Bar. The alarm view related to the event appears. Refer to "Alarm View Display" on page 97.

6.4 System Log Events Subview

The System Log Events subview is a default subview of the Network Events view. The System Log Events view shows the system logs received from the managed devices on the network. It is shown in the following figure.

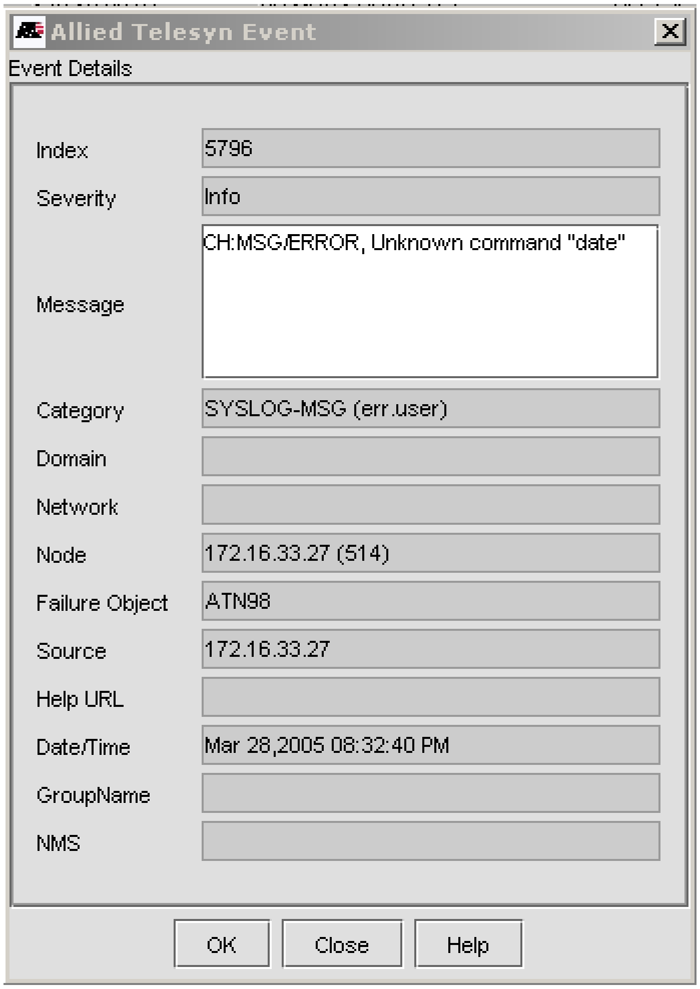


Date/Time	Source	Message	Category
Mar 28,2005 08:32:40 PM	172.16.33.27	CH:MSG/INFO, Configuration updated	SYSLOG-MSG (notice.user)
Mar 28,2005 08:32:40 PM	172.16.33.27	CH:MSG/ERROR, Unknown command "date"	SYSLOG-MSG (err.user)
Mar 28,2005 08:31:20 PM	172.16.33.29	CH:MSG/ERROR, SWITCH module unavailable on this product	SYSLOG-MSG (err.user)
Mar 28,2005 08:31:20 PM	172.16.33.29	CH:MSG/INFO, Configuration updated	SYSLOG-MSG (notice.user)
Mar 28,2005 08:31:19 PM	172.16.33.29	CH:MSG/ERROR, Unknown command "date"	SYSLOG-MSG (err.user)
Mar 28,2005 08:31:05 PM	172.16.33.26	CH:MSG/ERROR, SWITCH module unavailable on this product	SYSLOG-MSG (err.user)
Mar 28,2005 08:31:04 PM	172.16.33.26	CH:MSG/INFO, Configuration updated	SYSLOG-MSG (notice.user)
Mar 28,2005 08:31:04 PM	172.16.33.26	CH:MSG/ERROR, Unknown command "date"	SYSLOG-MSG (err.user)
Mar 28,2005 08:30:22 PM	172.16.33.19	Mar 29 09:07:59 Dot19 tAllegro: CLI001 7159 User: "officer" at IP: "172.16.65.3...	SYSLOG-CLI (info.local2)
Mar 28,2005 08:30:09 PM	172.16.33.19	Mar 29 09:07:46 Dot19 tAllegro: CLI001 7150 User: "officer" at IP: "172.16.65.3...	SYSLOG-CLI (info.local2)
Mar 28,2005 08:29:00 PM	172.16.33.11	Mar 28 20:59:52 Dot11 tAllegro: ID:CLI001 3866 User: "officer" at IP: "172.16.65...	SYSLOG-CLI (info.local2)
Mar 28,2005 08:28:41 PM	172.16.33.13	Mar 28 19:54:58 tAllegro: ID:CLI001 9316 User: "officer" at IP: "172.16.65.32" e...	SYSLOG-CLI (info.local2)
Mar 28,2005 08:28:40 PM	172.16.33.13	Mar 28 19:54:57 tAllegro: ID:CLI001 9307 User: "officer" at IP: "172.16.65.32" e...	SYSLOG-CLI (info.local2)
Mar 28,2005 08:28:16 PM	172.16.33.20	Mar 29 00:13:44 tAllegro: ID:CLI001 0590 User: "officer" at IP: "172.16.65.32" e...	SYSLOG-CLI (info.local2)
Mar 28,2005 08:28:15 PM	172.16.33.20	Mar 29 00:13:44 tAllegro: ID:CLI001 0580 User: "officer" at IP: "172.16.65.32" e...	SYSLOG-CLI (info.local2)

FIGURE 6-9 System Log Events Subview

The logs that are displayed in this view are configured using the System Log Configuration tool.

You can view detailed information on a log by right-clicking the log, and then selecting *Details* from the pop-up menu. An alternative method is to select the log, and then select *View* -> *Details* from the Panel-Specific Menu. In either case, the Event viewer will appear as shown in the following figure.



Event Details

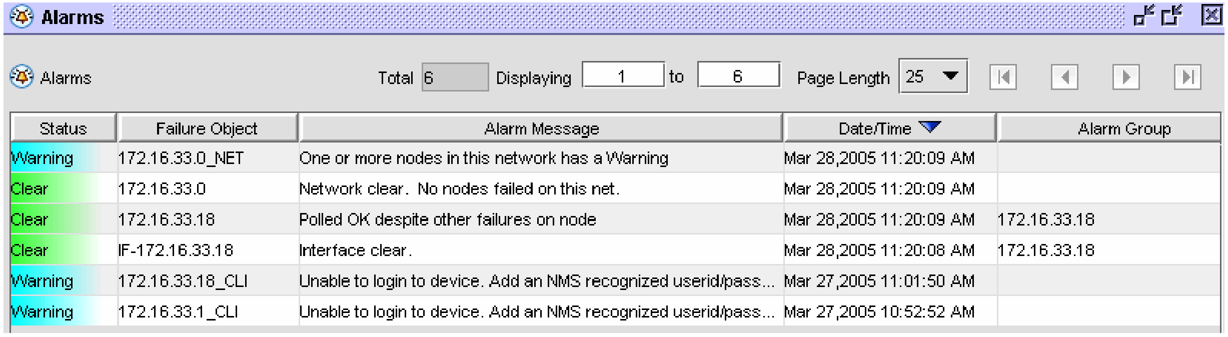
Index	5796
Severity	Info
Message	CH:MSG/ERROR, Unknown command "date"
Category	SYSLOG-MSG (err.user)
Domain	
Network	
Node	172.16.33.27 (514)
Failure Object	ATN98
Source	172.16.33.27
Help URL	
Date/Time	Mar 28,2005 08:32:40 PM
GroupName	
NMS	

FIGURE 6-10 Log Event Details Window - File

You can create custom views and event parsers for system logs in the same way you create them for Network Events. You can also save the log information to a file by selecting *Actions->Save To File* from the Panel-Specific Menu Bar or by clicking the **Save** icon in the Toolbar.

6.5 Alarm View Display

The Alarm View displays alarm information on your network. To access the Alarm View, select the node Alarms from the NMS Tree. An example of the Alarms View display is shown in the following figure.



Total 6 Displaying 1 to 6 Page Length 25

Status	Failure Object	Alarm Message	Date/Time	Alarm Group
Warning	172.16.33.0_NET	One or more nodes in this network has a Warning	Mar 28,2005 11:20:09 AM	
Clear	172.16.33.0	Network clear. No nodes failed on this net.	Mar 28,2005 11:20:09 AM	
Clear	172.16.33.18	Polled OK despite other failures on node	Mar 28,2005 11:20:09 AM	172.16.33.18
Clear	IF-172.16.33.18	Interface clear.	Mar 28,2005 11:20:08 AM	172.16.33.18
Warning	172.16.33.18_CLI	Unable to login to device. Add an NMS recognized userid/pass...	Mar 27,2005 11:01:50 AM	
Warning	172.16.33.1_CLI	Unable to login to device. Add an NMS recognized userid/pass...	Mar 27,2005 10:52:52 AM	

FIGURE 6-11 Alarm View Main Panel

Navigating the view is the same for all views and is described in "Navigating in a View" on page 90. Searching for information in the view is also the same and is described in "Searching in a View" on page 90.

6.5.1 Panel-Specific Menus for the Alarms View

When the Alarms view is displayed in the NMS Display Panel, the following menu items appear in the Panel-Specific Menu Bar that are specific to the Network Events view:

- *Edit* - Provides editing functions for the view. Items include:
  - *Configure* - Provides configuration functions for trap and event parsers, and for event filters.
  - *Delete* - Deletes the selected alarm.
  - *Pick Up/UnPick* - Assigns or unassigns ownership of the selected alarm to you.
  - *Clear* - Clears the selected alarm.
  - *Search* - Provides a search function for the view (refer to "Searching in a View" on page 90).
  - *Export Table Data* - Provides an export function for all of the view data. The data may be exported to a file (in delimited tabular form) or to a Web browser. The data may also be filtered.
  - *Export Selected Rows* - Provides an export function for selected rows in the view data.
  - *Schedule Alert Export* - The Alarms in the View can be exported to a file now or at a later time. The form for this function is the similar to the Schedule Event Export, and is explained in subsection "Schedule Event Export" on page 88.
- *View* - Provides additional display functions for the view. Items include:
  - *Alert Details* - Brings up the Alarm Details Form, as explained in "Specify Alarm Details" on page 99.
  - *Source Details* - Brings up the Details Form, except as follows:

    - For a port alarm, brings up the Port Details tabbed form.

    - For the VLAN IF, the Chassis View appears.

    - For the iMG/RG, the Triple Play Service Management Form appears
  - *Alarms* - Provides alarm information specific to the selected event.
- *Actions* - Provides a *Save To File* option, which saves the event information to a file.
- *Export Alerts* - Export to a file the rows displayed or all rows associated with the current view.

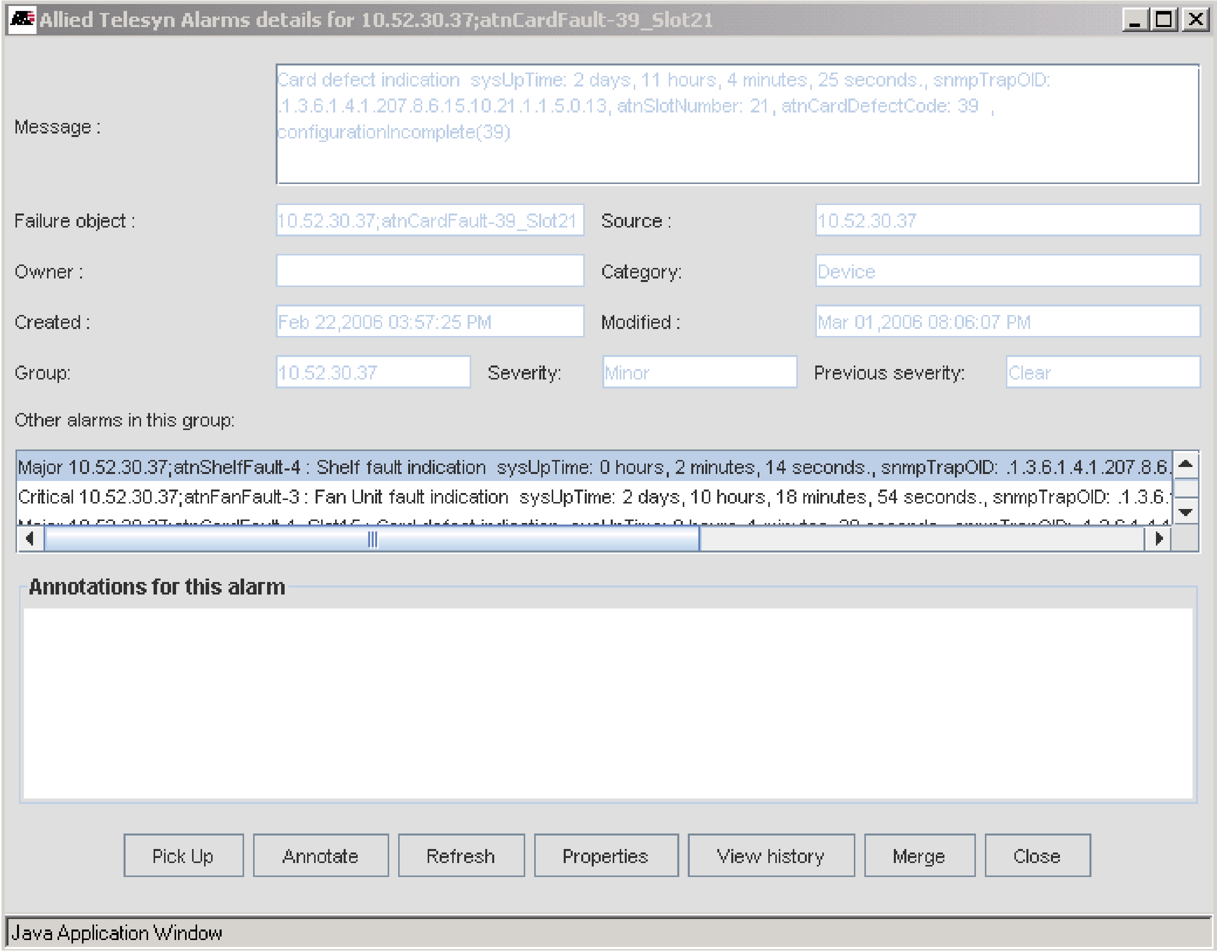
6.6 Creating Custom Views for Alarms

Refer to "Alarms" on page 1080 for a list of properties that are commonly used to create meaningful custom views.

6.7 Alarm View Tasks

6.7.1 Specify Alarm Details

By double-clicking or right clicking an alarm, you can view the complete details of the alarm. You can also select *View-> Details* from the Panel-Specific Menu Bar after selecting an alarm from the Alarm Viewer. (The selected alarm entry will turn a dark gray.) This brings up the alarm details form, as shown in the following figure.



Allied Telesyn Alarms details for 10.52.30.37;atnCardFault-39_Slot21

Message : Card defect indication sysUpTime: 2 days, 11 hours, 4 minutes, 25 seconds., snmpTrapOID: .1.3.6.1.4.1.207.8.6.15.10.21.1.1.5.0.13, atnSlotNumber: 21 , atnCardDefectCode: 39 , configurationIncomplete(39)

Failure object :	10.52.30.37;atnCardFault-39_Slot21	Source :	10.52.30.37		
Owner :		Category:	Device		
Created :	Feb 22,2006 03:57:25 PM	Modified :	Mar 01,2006 08:06:07 PM		
Group:	10.52.30.37	Severity:	Minor	Previous severity:	Clear

Other alarms in this group:

Major 10.52.30.37;atnShelfFault-4 : Shelf fault indication sysUpTime: 0 hours, 2 minutes, 14 seconds., snmpTrapOID: .1.3.6.1.4.1.207.8.6.

Critical 10.52.30.37;atnFanFault-3 : Fan Unit fault indication sysUpTime: 2 days, 10 hours, 18 minutes, 54 seconds., snmpTrapOID: .1.3.6.

Annotations for this alarm

FIGURE 6-12 Alarm Details Form

The following table lists the properties.

TABLE 6-2 Properties for Alarm Details

Property	Description for Alarm Detail Properties
Message	Important additional information regarding the alarm.
Failure object	Information about the specific entity, which has caused the alarm within the source as identified by the source field of the alarm.
Source	Information about the source of the alarm.
Owner	The name of the owner with which the alarm is associated.
Category	The category of the alarm.

TABLE 6-2 Properties for Alarm Details

Property	Description for Alarm Detail Properties
Created	The date and time when the alarm was first created.
Modified	The date and time when the alarm was last modified.
Severity	The criticality of the alarm.
Previous severity	The previous severity.

On the alarm details screen are buttons that provide the following (left to right):

- **Pickup**

  Clicking this annotates the alarm with the id of the user, so that others can see who is working the problem. The option then toggles to Unpick so that the user can remove the id later.

- **Annotate** (Alarm Annotations)

  Clicking this allows you to add notes for an alarm so that other users can see how this type of problem was solved, allowing for more efficient problem resolution.

- Refresh

  Clicking this refreshes the information on the form.

- **Properties**

  Clicking this opens a small window containing any user property that you have included for the alarm. This is actually non-editable and helps only to view the properties you have specified.

- **View history**

  Clicking this allows you to view the status of alarms added, updated, or deleted. NMS automatically takes care of updating, clearing, and deleting Alarm History.

- **Merge**

  Clicking this allows you to simultaneously view both Alarm Annotations and Alarm History by choosing the Merge option.

- Close

  Clicking this closes the window.

6.7.2 Configuring Alarm Filters

Alert filters are used to filter and modify the properties of an incoming alert. When the alert matches specified criteria, an action (such as sending an email) will occur.

To parse alarms, select *Edit* -> *Configure* > *Alarm Filters* from the Panel-Specific Menu Bar for Network Events. The Alert Filter Configuration form appears.

6.7.3 Saving Alarms to a File

Saving alarm information to a file is similar to saving network event information to a file, which is described in "Saving Events to a File" on page 93.

6.7.4 Viewing Related Events

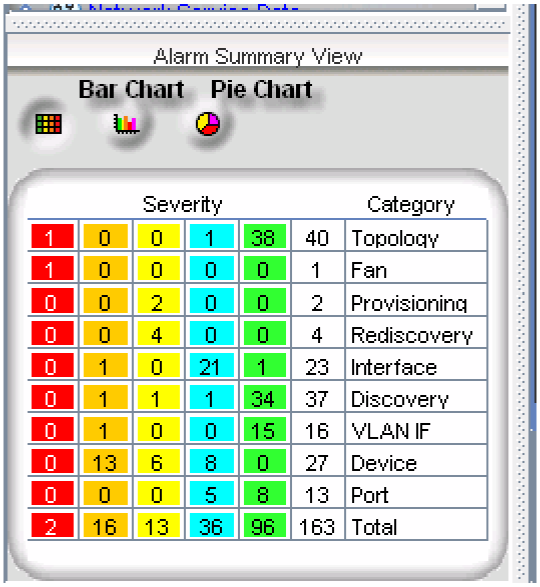
To view the related events for a specific alarm, select the alarm anywhere in its row, and then select *View -> Events* from the Panel-Specific Menu Bar. This displays the Event view panel and displays the events related to the alarm.

6.7.5 Clearing and Removing Alarms

Clearing alarms means to change the status of the alarm to Clear. Highlight the alarm (or alarms using the Ctrl key), and then select *Edit -> Clear* from the Panel-Specific Menu Bar. To remove the alarms from the database so that they will not be reported, highlight the alarm, and then select *Edit -> Delete* from the Panel-Specific Menu Bar.

6.7.6 Alarm Count Panel

The Alarm Count Panel provides a way to view the summary of the Alarms generated by the NMS. The summary gives the number of Alarms that have been generated under various categories and severity levels, as shown in the following figure.



Severity						Category
1	0	0	1	38	40	Topology
1	0	0	0	0	1	Fan
0	0	2	0	0	2	Provisioning
0	0	4	0	0	4	Rediscovery
0	1	0	21	1	23	Interface
0	1	1	1	34	37	Discovery
0	1	0	0	15	16	VLAN IF
0	13	6	8	0	27	Device
0	0	0	5	8	13	Port
2	16	13	36	96	163	Total

FIGURE 6-13 Alarm Count Panel

The Alarm Count Panel displays the Alarms generated in a tabular fashion to facilitate easy viewing. You can also see the alarm numbers in bar code and pie chart format.

Each row corresponds to a specific Application of Alarms. The Applications that are to be displayed in the Panel are configurable. Thus, the number of rows corresponds to the number of Applications of Alarms that have been configured to be viewed (excluding the last row that gives the Totals). An alarm will have a Severity; - Critical, Major, Minor, Warning, Clear. So, the number of columns corresponds to the number of Severity levels configured (excluding the last column that highlights the Application Name).

The Alarm count is done based on severity and when an Alarm is generated. The count is updated automatically under the appropriate column (Severity).

The last row gives the total count of Alarms of all applications (including the ones without any application defined) classified into different severity levels.

7. File Administration

Many administrative tasks for the AlliedView NMS are done by adding, changing, and deleting files on the server. However, directly accessing these files should not be attempted, since a loss of AlliedView NMS functionality could result.

The NMS provides GUI-based functions that make updating the AlliedView NMS files easy and less error-prone. Moreover, the server does not have to be restarted for the changes to take effect. However, a few tasks do involve restarting the server. These tasks are included and the point at which a restart is required is highlighted.

For AT and iMAP devices, you are able to change the default prompt to a custom string on the device. For AT devices, the default ">" at the end of the prompt is required for the NMS to discover these devices.

In this document <NMS_HOME> refers to the directory where the NMS is installed. The default in the installation wizard is:

- Windows Server 2003/2008, XP, 7 (32-bit OS) - **c:\Program Files\Allied Telesis\AlliedView NMS**
- Windows Server 2003/2008, XP, 7 (64-bit OS) - **c:\Program Files (x86)\Allied Telesis\AlliedView NMS**
- Linux - **/opt/AlliedTelesis/AlliedViewNMS**

Directory names inside configuration files use the Internet standard of forward slashes (/) on both Windows and Linux platforms.

Table 7-1 lists the tasks that are fully supported. Accessing a file on the server and changing a value without Allied Telesis Support could result in a loss of AlliedView NMS functionality.

TABLE 7-1 Task List for File Administration

Task	Screen / Form Name (if Applicable)	Section
Discovery Configurator (Service Provider Edition)	Form with set of Tabs for SE version Schedule Tab SNMP Tab CWMP Tab CLI Logins Tab Network Discovery Tab Node Discovery Tab Other Discovery Tab	"Discovery Configurator" on page 104, "Discovery Configurator - Service Provider Edition" on page 105 "Schedule Tab" on page 105 "SNMP Tab" on page 106 "CWMP Tab" on page 107 "CLI Logins Tab" on page 109 "Network Discovery Tab" on page 112 "Node Discovery Tab" on page 114 "Other Discovery Tab" on page 116
Discovery Configurator (Enterprise Edition)	Form with set of Tabs for EE version Basic Tab SNMP CWMP Tab CLI Logins Tab Network Discovery Tab Node Discovery	"Discovery Configurator" on page 104, "Discovery Configurator - Enterprise Edition" on page 117 "Basic Tab" on page 118 "SNMP Tabs" on page 119 "CWMP Tab" on page 120 "CLI Logins Tab" on page 120 "Network Discovery Tab" on page 123 "Node Discovery Tab" on page 124
Add Network or Node	Allied Telesis Add Network, Add Node	"Adding a Network or Node from the Network Inventory" on page 125

TABLE 7-1 Task List for File Administration (Continued)

Task	Screen / Form Name (if Applicable)	Section
Backup and Restore	AlliedView NMS Backup AlliedView NMS Restore Device Backup Limit	"AlliedView NMS Backup (On Demand)" on page 126 "Restore the AlliedView NMS (GUI Screens)" on page 129 "Device Backup (Per-Device Limit)" on page 131
Inventory Report	Inventory Management	"Inventory Reporting" on page 131
Node Limiting, Registering NMS load	AlliedView NMS License Manager	"AlliedView NMS License Manager" on page 136
Software Downloads	Software Configuration (Modify Release Configuration, Create Custom Load buttons)	"File Keys to Identify Downloadable Files" on page 141
Monitor AlliedView NMS server/processes	Status Monitoring	"Status Monitoring" on page 143
Firmware Upload Tool	Load Import	"Downloading Device Files" on page 148

7.1 Discovery Configurator

The NMS uses the Discovery Configurator to discover devices in a network. To access the Discovery Configurator within the NMS client, from the main menu go to **Tools > Discovery Configurator**.

On the NMS server you can also access the Discovery Configurator as a standalone tool:

- Windows: Go to **Start > Allied View NMS > Tools > Discovery Configurator**.
- Linux: Execute the file **<NMS_home>/bin/admintools/DiscoveryConfigurator.sh**.

The general procedure to initially discover devices in a network is:

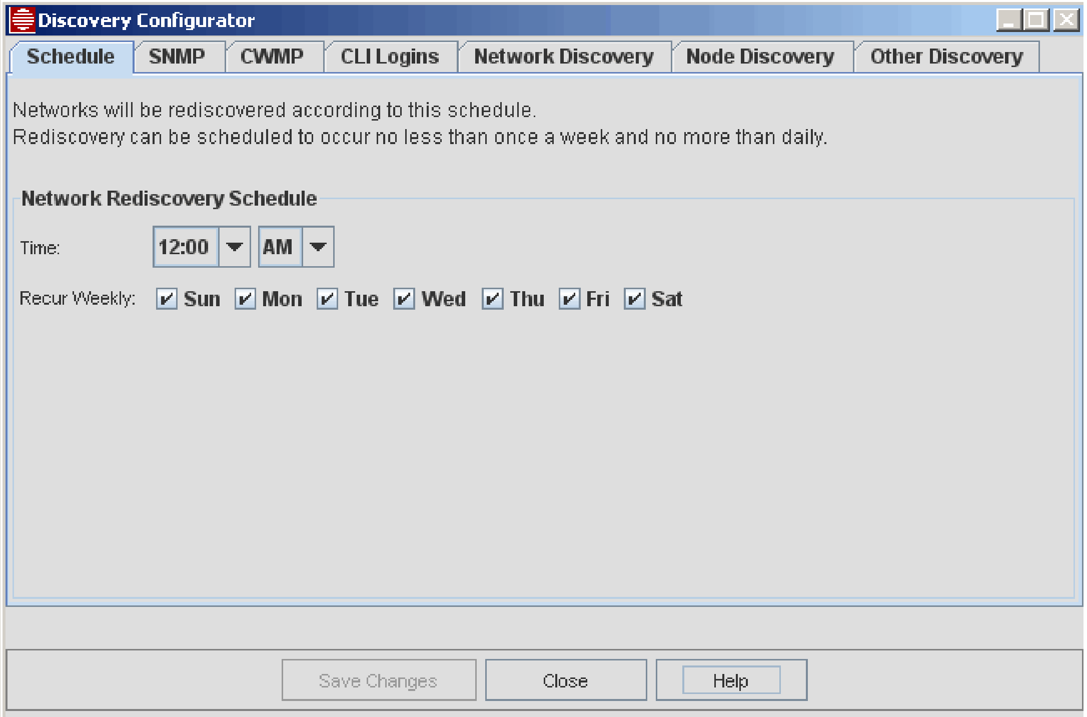
1. Using the tabs in the Discovery Configurator, set up the criteria for initial discovery. This includes the discovery schedule, global and per-device SNMP communities, CLI logins, and determining what specific networks and nodes to discover.
2. Click **Save Changes** to save the changes without closing the Discovery Configurator. Click **Close** to exit the tool.
3. If you have not yet started the NMS server, start up the NMS server by following the instructions in the *AlliedView NMS Installation Guide*.
4. Open the NMS client. Networks and devices appear in the NMS screens as they are discovered.

The Discovery Configurator is different for different versions of the NMS. For the Service Provider Edition, see "Discovery Configurator - Service Provider Edition" on page 105. For the Enterprise Edition, see "Discovery Configurator - Enterprise Edition" on page 117.

7.2 Discovery Configurator - Service Provider Edition

The Discovery Configurator includes seven tabs: **Schedule**, **SNMP**, **CWMP**, **CLI Logins**, **Network Discovery**, **Node Discovery**, and **Other Discovery**. Each of these tabs is described below.

7.2.1 Schedule Tab



Networks will be rediscovered according to this schedule.
Rediscovery can be scheduled to occur no less than once a week and no more than daily.

Network Rediscovery Schedule

Time: 12:00 AM

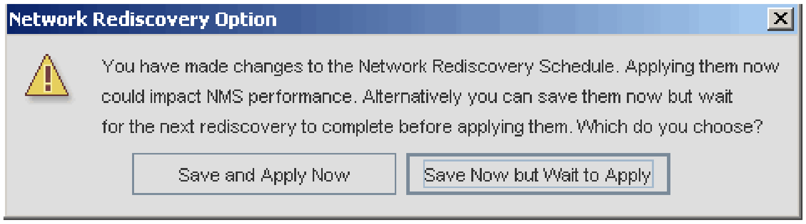
Recur Weekly: ☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

FIGURE 7-1 Discovery Configurator – Schedule Tab

The **Schedule** tab allows configuring the rediscovery time, the time all managed devices in networks included for discovery in the Network Discovery tab will be rediscovered to update the NMS database with any changes, including the addition of new devices. Devices in the Node Discovery tab will not be rediscovered.

To schedule the time, choose an hour and select one or more days of the week. Nightly rediscovery is recommended. At least once a week is required, with no more than once every 24 hours.

If a you make a change in the Network Rediscovery Schedule, the NMS displays a popup that requires you to select from two options: **Save and Apply Now** or **Save Now but Wait to Apply**.



You have made changes to the Network Rediscovery Schedule. Applying them now could impact NMS performance. Alternatively you can save them now but wait for the next rediscovery to complete before applying them. Which do you choose?

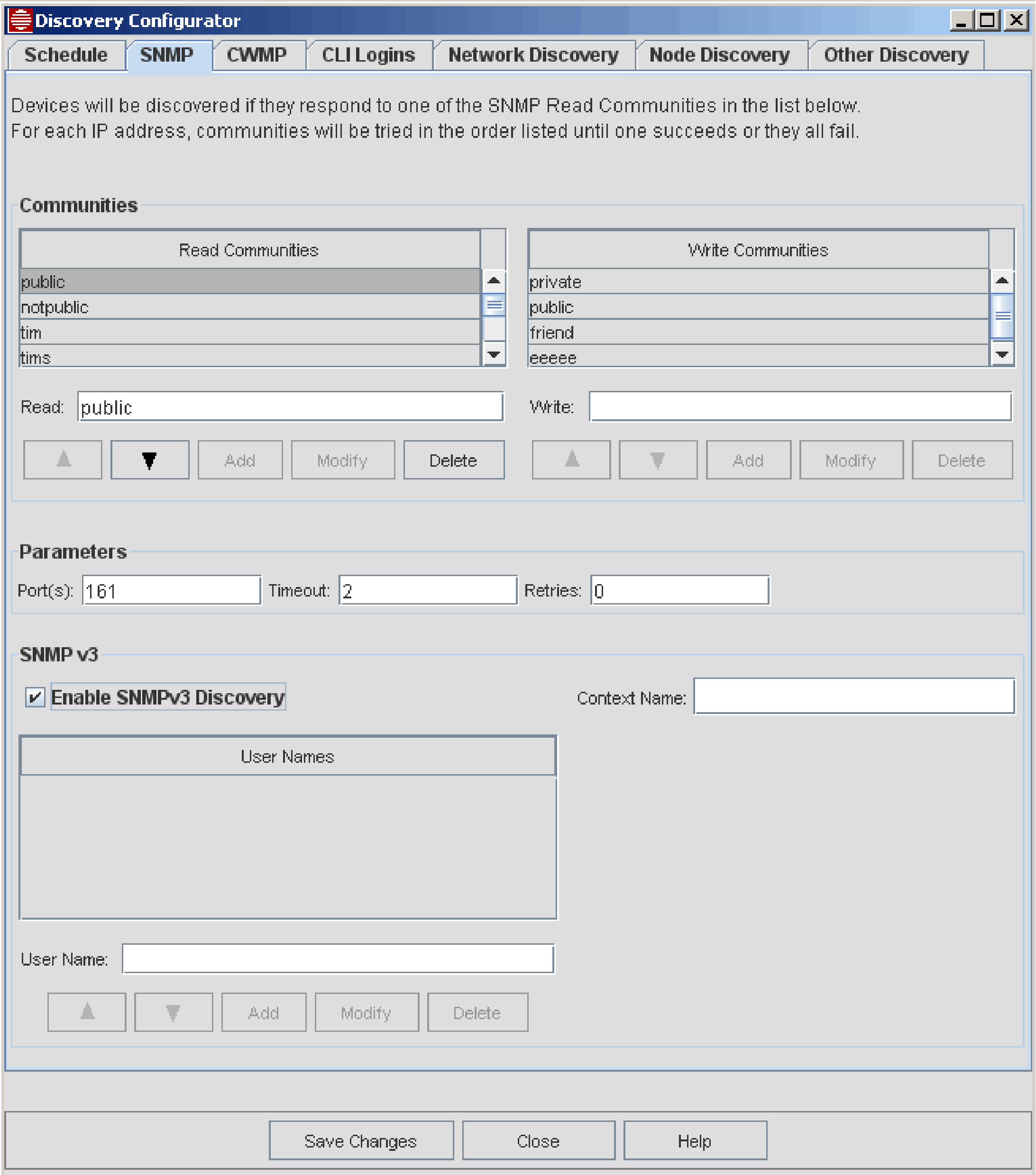
FIGURE 7-2

- Selecting **Save and Apply Now** restarts discovery and applies the changes immediately. This may slow down the NMS and temporarily disrupt operations.

- Selecting **Save Now but Wait to Apply** postpones applying the schedule changes until the next discovery on the current schedule completes. This avoids unnecessary disruptions to the NMS.

When you add a new network discovery happens immediately with either option since the network has not been previously discovered.

7.2.2 SNMP Tab



Devices will be discovered if they respond to one of the SNMP Read Communities in the list below.
For each IP address, communities will be tried in the order listed until one succeeds or they all fail.

Communities

Read Communities
public
notpublic
tim
tims

Write Communities
private
public
friend
eeeee

Read: public

Write:

Parameters

Port(s): 161 Timeout: 2 Retries: 0

SNMP v3

☑ Enable SNMPv3 Discovery

Context Name:

User Names

User Name:

FIGURE 7-3 Discovery Configurator – SNMP Tab

Only devices that respond to SNMP can be discovered and managed by the AlliedView NMS. The NMS will perform “SNMP Ping” operations with each of the given read communities until a device responds or all communities have been tried and failed. (SNMP Pings are essentially SNMP get requests for selected system variables. Devices that respond are considered “connected” and those that don't are considered “unreachable”)

7.2.2.1 SNMPv2

For most devices, only read communities are used during discovery. Some devices, including iMG/RGs, require discovering write communities as well.

Communities will be attempted in the order displayed. The order may be modified by selecting a row and then clicking on the up/down buttons.

Communities may be added, modified, or deleted with the **Add**, **Modify** or **Delete** Buttons. The Add button will add to the list whatever is in the Read or Write text field. The Modify button will replace whatever is in the selected row with whatever has been typed in the Read or Write text field.

The SNMP agent port, timeout, and retry count can be configured as well. The defaults are 161, 2, and 0 respectively. Whereas 161 is the most commonly used SNMP agent port, others can be added as a space-separated list. Each port will be tried in the given order.

7.2.2.2 SNMPv3

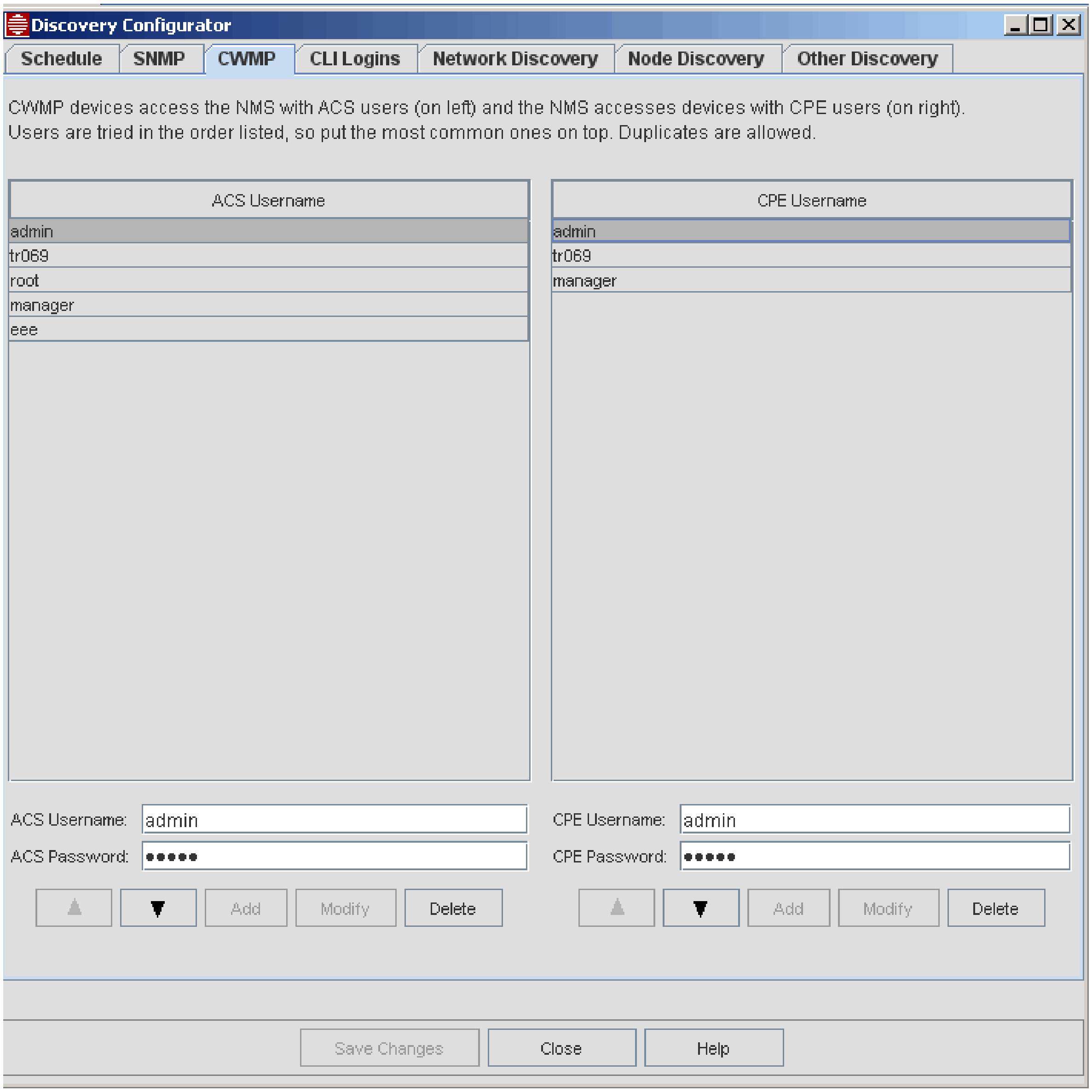
There is the option to enable SNMPv3 Discovery, which adds security and administration features. (For information on the relationships between the SNMP versions refer to RFC 3416.)

The SNMP panel allows the addition of Users following the User-based security model defined in RFC 3414. As RFC 3416 states, only those principals (users) having legitimate rights can access or modify the values of any MIB objects supported by that entity.

The SNMP panel includes the Enable SNMPv3 Discovery option, as shown in Figure 7-4. User Names are added by typing in the User Name field, the Context Field, and then selecting **Add**. Names can continue to be added and the order changed using the direction arrows. A name can be modified by selecting a name, changing the name in the User name field, and selecting **Modify**. Selecting **Save Changes** writes the values to the NMS.

7.2.3 CWMP Tab

The **CWMP** (Common WAN Management Protocol) tab addresses TR-069 support. This tab allows you to set ACS (Auto Configuration Server) and CPE (Customer Premise Equipment) login credentials for iMGs. The ACS login credentials are used by iMGs when they connect to the ACS embedded with the NMS server. The NMS uses the credentials in the CPE list during discovery to connect with an iMG. The credentials in each list are tried in the order they are listed. Duplicate usernames with different passwords are allowed in each list.



CWMP devices access the NMS with ACS users (on left) and the NMS accesses devices with CPE users (on right).
Users are tried in the order listed, so put the most common ones on top. Duplicates are allowed.

ACS Username
admin
tr069
root
manager
eee

CPE Username
admin
tr069
manager

ACS Username: admin
ACS Password: ●●●●●

CPE Username: admin
CPE Password: ●●●●●

FIGURE 7-4 Discovery Configurator – CWMP Tab

To add a new credential:

1. In the **ACS Username** or **CPE Username** field, enter a valid username.
2. In the **ACS Password** or **CPE Password** field, enter the password associated with the username.
3. Click **Add**.

To modify a credential:

1. In the ACS or CPE list, select the row of the credential you want to change.
2. Enter the new username or password in the username or password field below the list.
3. Click **Modify**.

To delete a credential:

1. In the ACS or CPE list, select the row of the credential you want to delete.

2. Click **Delete**.

To change the order of the credentials:

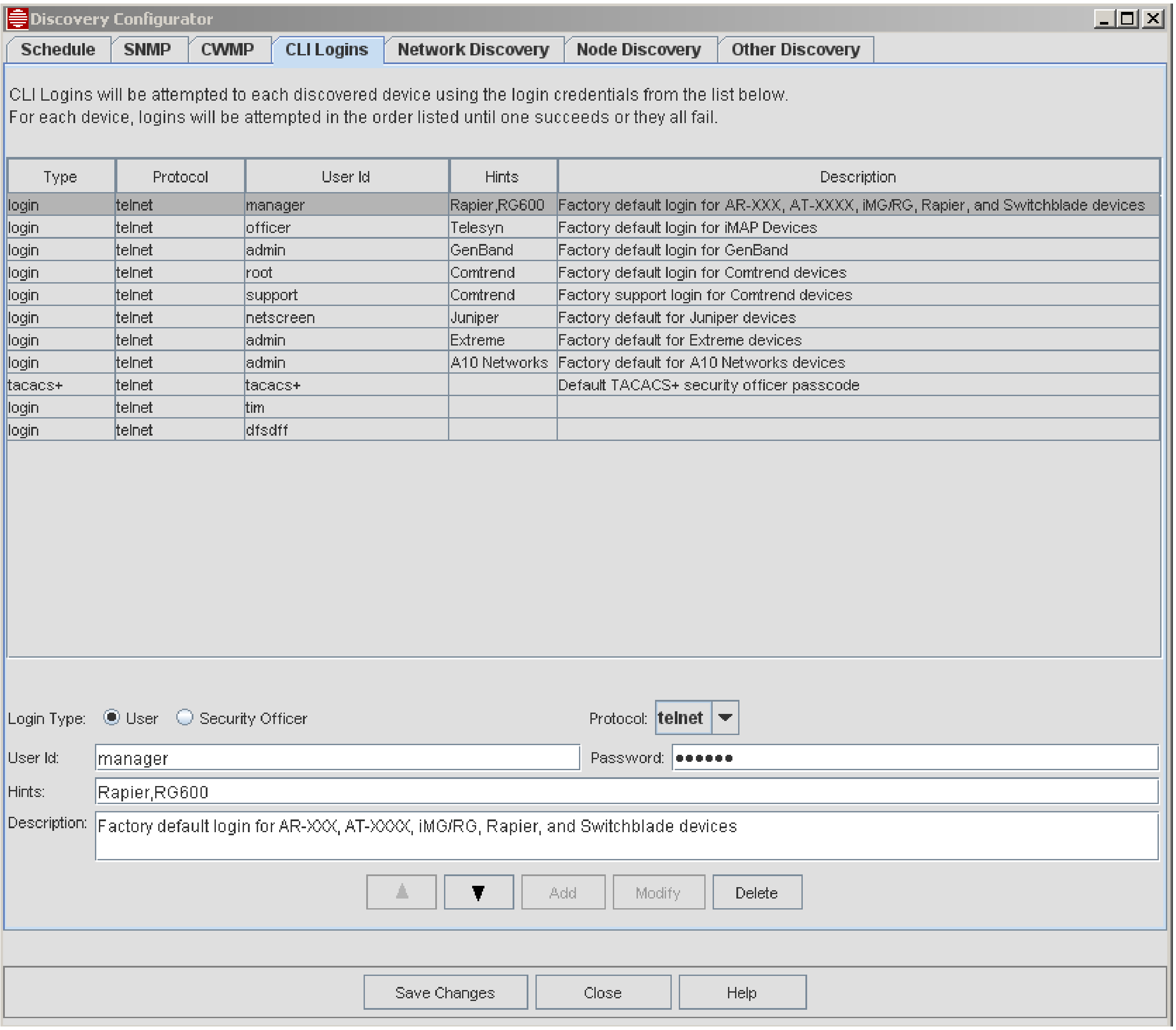
1. In the ACS or CPE list, select the row of the credential you want to move.
2. Click the up (▲) or down (▼)arrow below the list to change the location of the credential in the list.

7.2.4 CLI Logins Tab

The CLI Login Manager allows you to specify a list of CLI username/password pairs that will be used by the discovery process to determine the CLI username and password for individual devices. The username and password discovered for each device are used for all CLI interactions with the device.

All managed devices are shipped with a factory-default CLI username and password. For security purposes, you should change these as soon as you install a device.

Caution: All NMS users use the username and password to access the device. To enable NMS users to query and control a device, the device name and password must be at a security officer level. Failure to do so may make certain operations performed at the NMS on a device to fail.



CLI Logins will be attempted to each discovered device using the login credentials from the list below.
For each device, logins will be attempted in the order listed until one succeeds or they all fail.

Type	Protocol	User Id	Hints	Description
login	telnet	manager	Rapier,RG600	Factory default login for AR-XXX, AT-XXXX, iMG/RG, Rapier, and Switchblade devices
login	telnet	officer	Telesyn	Factory default login for iMAP Devices
login	telnet	admin	GenBand	Factory default login for GenBand
login	telnet	root	Comtrend	Factory default login for Comtrend devices
login	telnet	support	Comtrend	Factory support login for Comtrend devices
login	telnet	netscreen	Juniper	Factory default for Juniper devices
login	telnet	admin	Extreme	Factory default for Extreme devices
login	telnet	admin	A10 Networks	Factory default for A10 Networks devices
tacacs+	telnet	tacacs+		Default TACACS+ security officer passcode
login	telnet	tim		
login	telnet	dfsdff		

Login Type: ● User ○ Security Officer Protocol: telnet

User Id: manager Password: ●●●●●●

Hints: Rapier,RG600

Description: Factory default login for AR-XXX, AT-XXXX, iMG/RG, Rapier, and Switchblade devices

FIGURE 7-5 Discovery Configurator – CLI Logins Tab

Once a device has been discovered by SNMP, more detailed discovery requiring a CLI login is required to manage the device. The NMS attempts to log into each device until it either discovers an accepted login or all login attempts are rejected. The login sequence generally follows the order of the logins in the table. The order may be modified by selecting a row and then clicking on the up or down ▲ ▼ buttons.

The login sequence can be overridden by the **Hints** field. Hints are a comma-separated list of device category, sysLocation, IP address, and subnets (in x.x.x.x/bits notation). Login parameters for a device that matches any of the hints will be attempted before any other login parameters. If there are more than 1 login entry with matching hints, they will be attempted in the sequence from the list.

The NMS will retry each user id up to 5 minutes if it gets connection-refused errors (in case it just came up and needs more time to finish initializing telnet and/or ssh services). If the NMS never gets connected, it will raise a discovery failure alarm.

If all login attempts with matching hints fail, all of the entries without hints will be attempted until one is accepted or all are rejected. And if all of those fail, all of the rest (without matching hints) will be attempted.

The Description field is a free format reminder of what each login entry represents.

There are 2 login types: User and Security Officer, which are specified by the radio buttons. The “user” type uses the User Id and Password to initially log into the device. User login is all that’s required for iMAPs running without TACPLUS.

If an iMAP is running with TACPLUS enabled, the NMS also needs a Security Officer passcode (to enable securityofficer). Security Officer passcodes can be designated by clicking on the Security Officer radio button. For Security Officer, the User Id field is not applicable and will be disabled and set to “tacacs+”. (You can still define a user login with the user id tacacs+, if necessary, by clicking on the User radio button instead of the Security Officer radio button) Security Officer passcodes will be attempted as ordered in the list and as overridden by Hints. Since multiple Security Officer passcodes are permissible, be sure to use the description field to keep track of which is which (since they will typically be indistinguishable without displaying the passcode).

Buttons specific to the CLI Login Manager are:

- **Add** - Adds a new entry to the CLI User list—after the current position of the selected login. (Duplicates are allowed)
- **Modify** - Overwrites the currently selected login with what’s in the main dialog.
- **Delete** - Deletes the currently selected login from the CLI User list.

Note: Discovery uses the CLI logins in the order specified in the CLI Login Manager. There is a performance hit associated with each failed login attempt. Use the up/down keys to order the list such that the most likely pair is listed first. (Use the Hints field to help identify device)

Caution: One feature for AT and iMAP devices is the ability to change their default prompts to a custom string. (For AT devices the default prompt is “>”, and for iMAP devices this feature begins with the default prompt “>>”.) Therefore, this default prompt should not be changed.

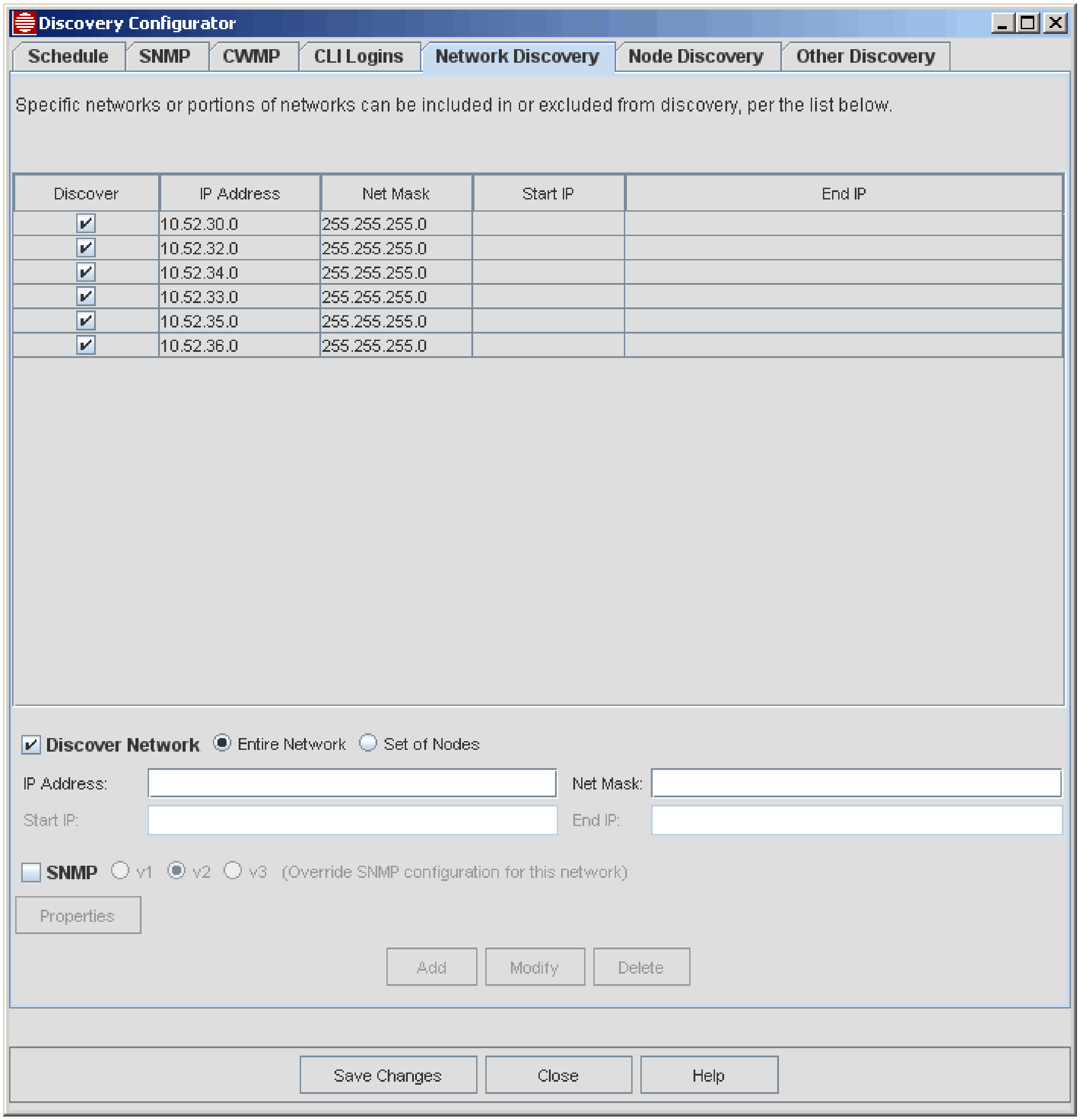
There is also the option to select the protocol. The default is telnet, but here is also the option to choose SSH. These are also added to the User ID list.

Most Allied Telesis devices support SSHv2. Using SSH involves configuring and enabling the SSH server. This involves:

- Server authentication, confidentiality, and integrity
- User authentication through the use of a password and/or public key
- Connection encryption for interactive login sessions

Refer to customer documents for Allied Telesis products for support of specific SSH features.

7.2.5 Network Discovery Tab



Specific networks or portions of networks can be included in or excluded from discovery, per the list below.

Discover	IP Address	Net Mask	Start IP	End IP
☑	10.52.30.0	255.255.255.0		
☑	10.52.32.0	255.255.255.0		
☑	10.52.34.0	255.255.255.0		
☑	10.52.33.0	255.255.255.0		
☑	10.52.35.0	255.255.255.0		
☑	10.52.36.0	255.255.255.0		

☑ Discover Network ● Entire Network ○ Set of Nodes

IP Address: Net Mask:

Start IP: End IP:

□ SNMP ○ v1 ● v2 ○ v3 (Override SNMP configuration for this network)

FIGURE 7-6 Discovery Configurator – Network Discovery Tab

This tab specifies networks to discover (or exclude from discovery). The discovery process will attempt to discover devices at all IP addresses in the network (or exclude all such addresses if configured for exclusion).

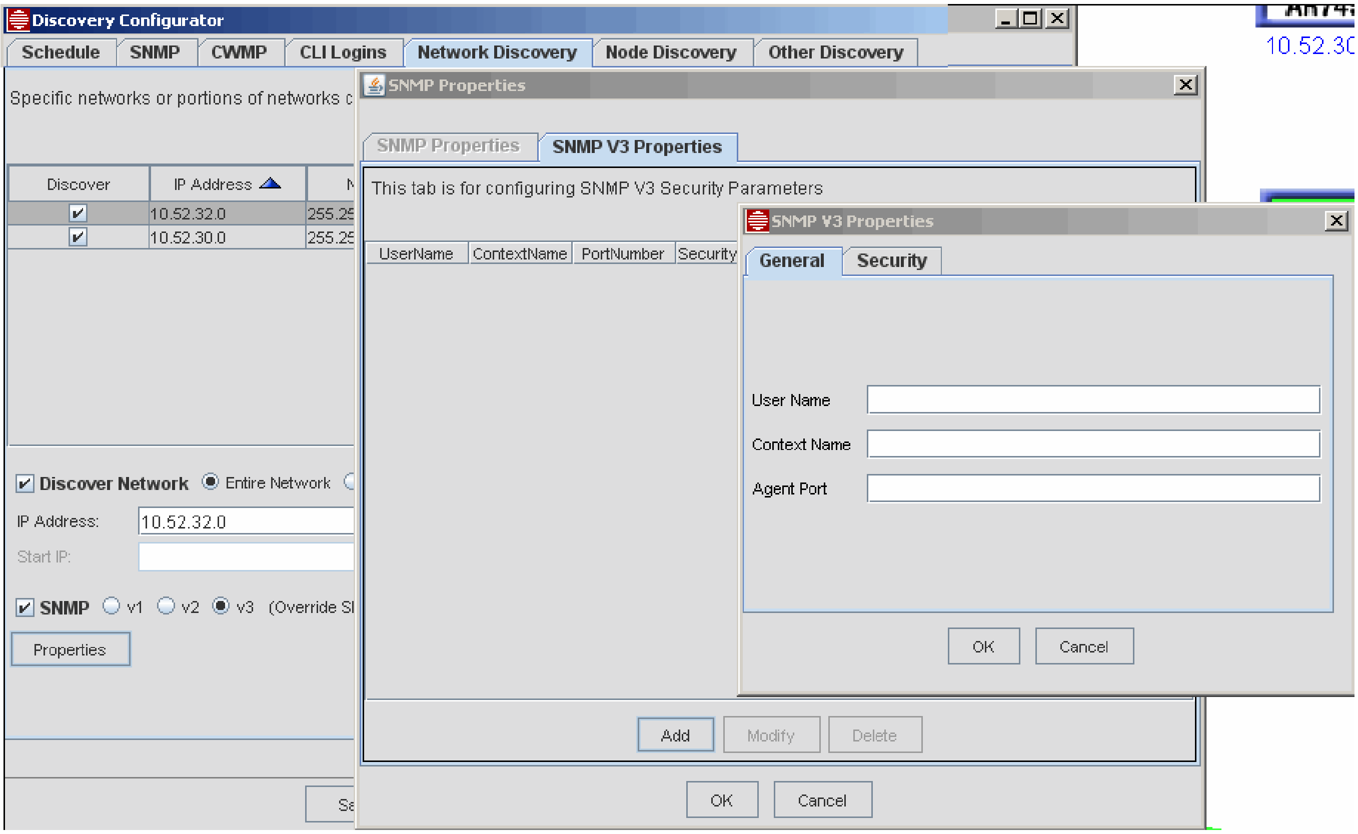
Networks can be added, modified, or deleted with the **Add**, **Modify**, and **Delete** buttons.

The “Discover Network” toggle, when checked, means to discover the network. When unchecked, that network will be ignored during discovery.

The “Entire Network” radio button, when selected means to use all addresses in the network, specified by the IP Address and Net Mask fields. When “Set of Nodes” is selected instead, only the addresses from the Start IP to the End IP will be discovered.

If SNMP discovery is enabled, network discovery will normally use the parameters configured on the SNMP tab, but they can be overridden for specific networks and subnets by selecting the SNMP option on this tab.The properties to fill in depend on the SNMP version selected.

A version of SNMP can be chosen to override what is configured for the network. After choosing the SNMP version, selecting the **Properties** button allows the parameters to be filled in. Refer to the following figure.



Discover	IP Address	N
☑	10.52.32.0	255.25
☑	10.52.30.0	255.25

This tab is for configuring SNMP V3 Security Parameters

☑ Discover Network ● Entire Network ○

IP Address: 10.52.32.0

Start IP:

☑ SNMP ○ v1 ○ v2 ● v3 (Override SI

FIGURE 7-7 Setting Properties for SNMPv3

All networks, including the local net, have to be added via the network tab.

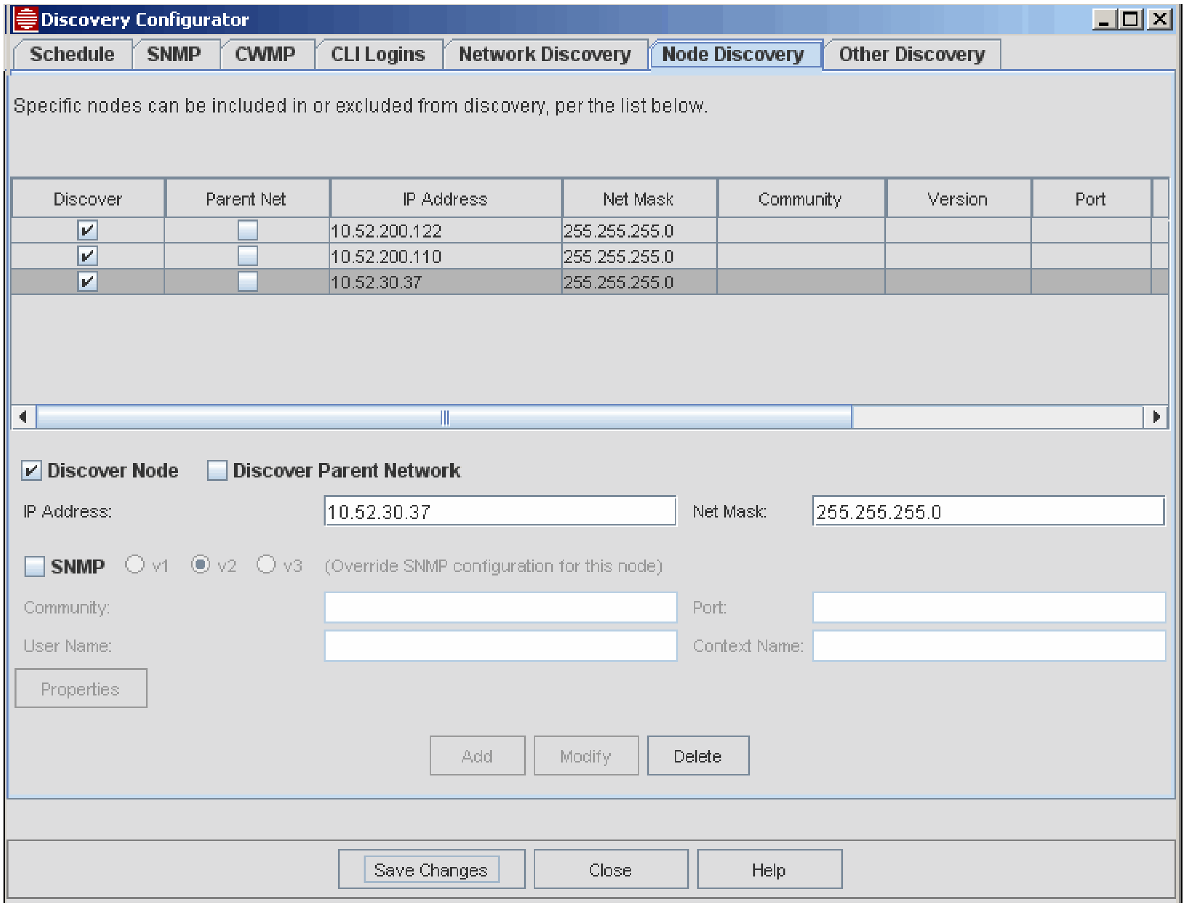
Caution: It is not possible to delete a network from discovery once discovery begins on that network. Discovery begins any time immediately after saving changes. Therefore, to permanently remove a network from the discovery configuration, shut down the NMS to shut down the discovery process and use the standalone Discovery Configurator to delete the unwanted network. Networks are successfully deleted, however, when deleted before saving changes.

The user can add networks and nodes in the Network Inventory screen as Managed Objects and this will take effect immediately. The menu choice:

- Network Inventory / Edit -> Add Network
- Network Inventory / Edit -> Add Node

brings up the dialog to add a network or node. Refer to "Adding a Network or Node from the Network Inventory" on page 125.

7.2.6 Node Discovery Tab



Specific nodes can be included in or excluded from discovery, per the list below.

Discover	Parent Net	IP Address	Net Mask	Community	Version	Port
☑	□	10.52.200.122	255.255.255.0			
☑	□	10.52.200.110	255.255.255.0			
☑	□	10.52.30.37	255.255.255.0			

☑ Discover Node □ Discover Parent Network

IP Address: 10.52.30.37 Net Mask: 255.255.255.0

□ SNMP ○ v1 ● v2 ○ v3 (Override SNMP configuration for this node)

Community: Port:

User Name: Context Name:

FIGURE 7-8 Discovery Configurator – Node Discovery Tab.

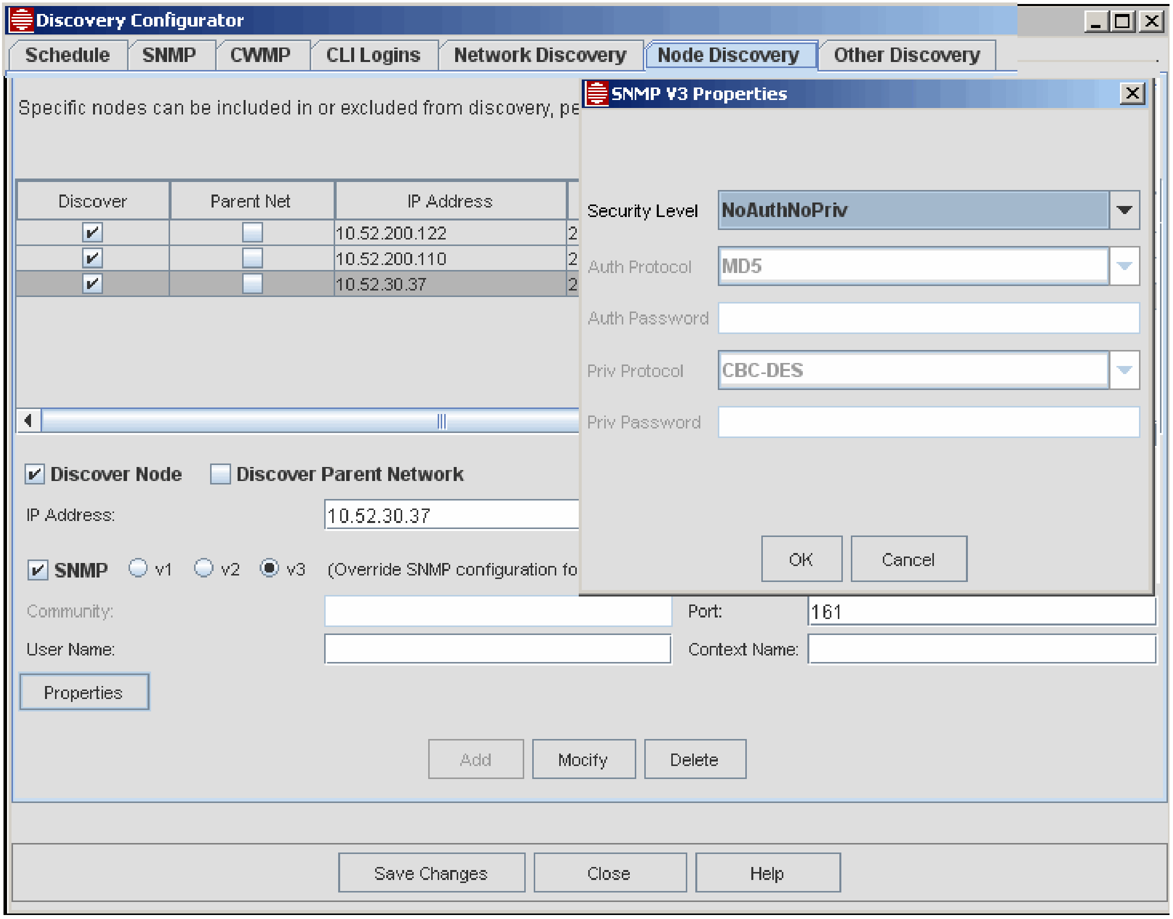
This tab specifies specific nodes to discover (or exclude from discovery).

Nodes can be added, modified, or deleted with the Add, Modify, and Delete buttons.

The “Discover Node” toggle, when checked, means to discover the node. When unchecked, that node will be ignored (excluded) from discovery.

The “Discover Parent Network” tab means to discover all the devices in the parent network, as well. The parent network will be considered to be all IP addresses in the same subnet as the node as defined by its IP Address and its Net Mask. When unchecked, only the one node will be discovered.

The SNMP version used can be selected here as well, with the properties determined by the version, as shown in the following figure.



Specific nodes can be included in or excluded from discovery, pe

Discover	Parent Net	IP Address	
☑	□	10.52.200.122	2
☑	□	10.52.200.110	2
☑	□	10.52.30.37	2

☑ Discover Node □ Discover Parent Network

IP Address: 10.52.30.37

☑ SNMP ○ v1 ○ v2 ● v3 (Override SNMP configuration fo

Community:

Port: 161

User Name:

Context Name:

Security Level: NoAuthNoPriv

Auth Protocol: MD5

Auth Password:

Priv Protocol: CBC-DES

Priv Password:

FIGURE 7-9 Setting Properties for SNMPv3

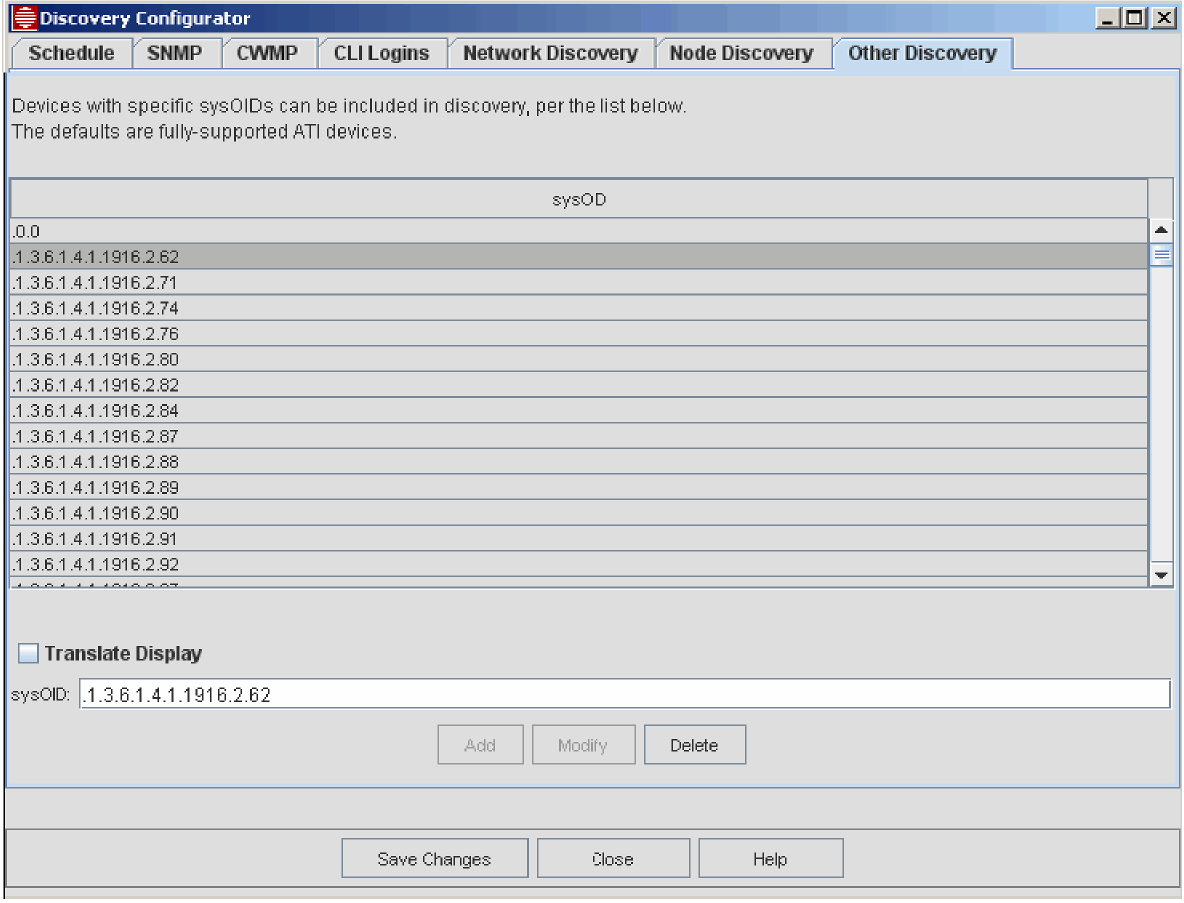
The user can add networks and nodes in the Network Inventory screen as Managed Objects and this will take effect immediately. The menu choice:

- Network Inventory / Edit -> Add Network
- Network Inventory / Edit -> Add Node

brings up the dialog to add a network or node. Refer to "Adding a Network or Node from the Network Inventory" on page 125.

Note: If nodes are failing initial discovery, change the "Retries" parameter (default 0) and the "Timeout" parameter from the SNMP Tab, and then use the ***Network Inventory / Edit -> Add Node*** *to retry initial discovery.*

7.2.7 Other Discovery Tab



Devices with specific sysOIDs can be included in discovery, per the list below.
The defaults are fully-supported ATI devices.

sysOD
.0.0
.1.3.6.1.4.1.1916.2.62
.1.3.6.1.4.1.1916.2.71
.1.3.6.1.4.1.1916.2.74
.1.3.6.1.4.1.1916.2.76
.1.3.6.1.4.1.1916.2.80
.1.3.6.1.4.1.1916.2.82
.1.3.6.1.4.1.1916.2.84
.1.3.6.1.4.1.1916.2.87
.1.3.6.1.4.1.1916.2.88
.1.3.6.1.4.1.1916.2.89
.1.3.6.1.4.1.1916.2.90
.1.3.6.1.4.1.1916.2.91
.1.3.6.1.4.1.1916.2.92

□ Translate Display

sysOID: .1.3.6.1.4.1.1916.2.62

FIGURE 7-10 Discovery Configurator – Other Discovery Tab

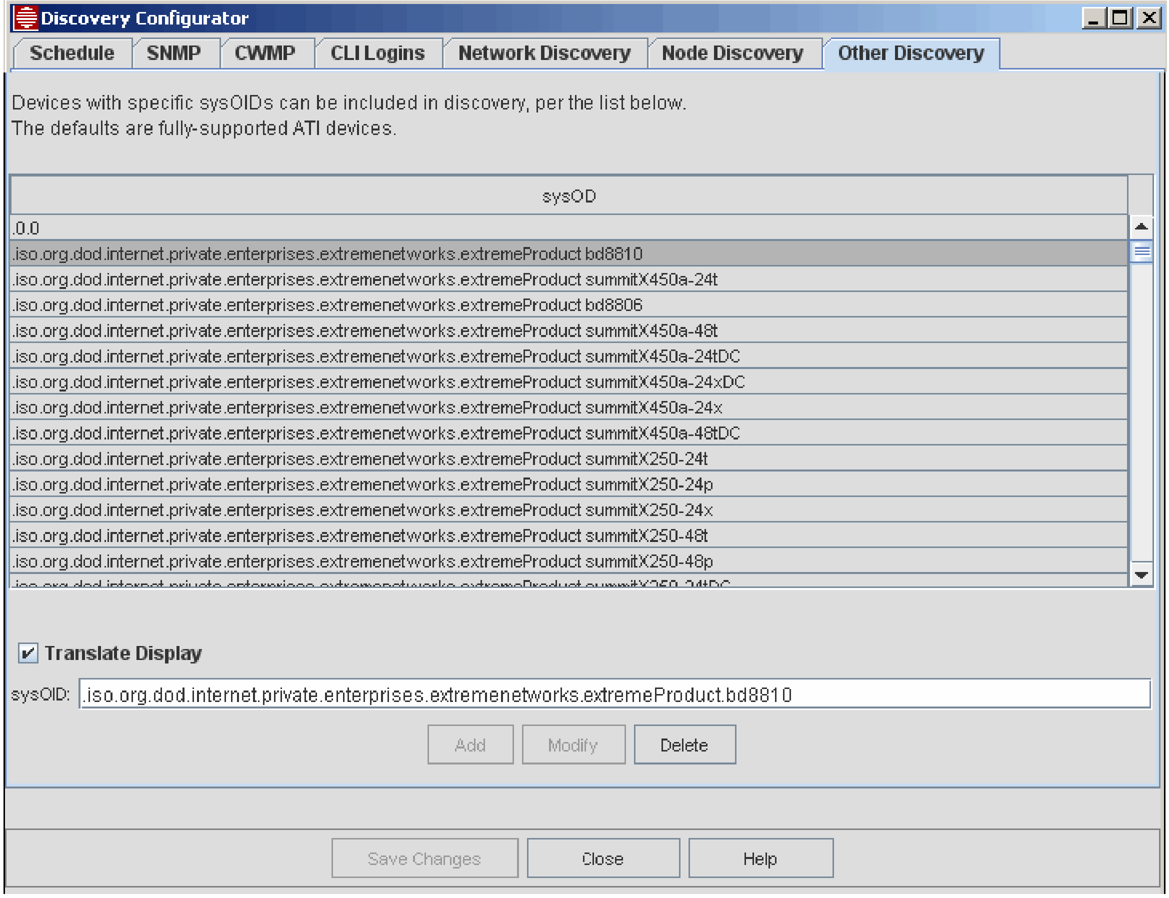
This tab lists sysOIDs (SNMP system Object Identifiers) of devices to be included for discovery. Any device discovered by way of SNMP will be rejected unless its sysOID is one of these from this table. The defaults for this table are the Allied Telesis devices fully-supported by the AlliedView NMS.

As shown below, the “Translate Display” toggle can be checked to display sysOIDs as translated names, provided the names are adequately defined by the MIBs installed with the AlliedView NMS. Names will be a mix of numbers and names where available MIBs are not complete. When unchecked, sysOIDs are displayed as instance identifiers (numbers only).

Additional sysOIDs can be added, modified, or deleted with the Add, Modify, and Delete buttons. Added sysOIDs can be displayed and minimally managed (live status monitoring, for example).

When adding or modifying sysOIDs, names or numbers may be entered into the sysOID text field whether or not the “Translate Display” toggle is selected. Names will be resolved to numbers if the appropriate MIBs are installed. Otherwise the user will be prompted to enter the sysOID in numeric form.

The default sysOIDs cannot be modified or deleted.



Devices with specific sysOIDs can be included in discovery, per the list below.
The defaults are fully-supported ATI devices.

sysOD
.0.0
.iso.org.dod.internet.private.enterprises.extremenetworks.extremeProduct.bd8810
.iso.org.dod.internet.private.enterprises.extremenetworks.extremeProduct.summitX450a-24t
.iso.org.dod.internet.private.enterprises.extremenetworks.extremeProduct.bd8806
.iso.org.dod.internet.private.enterprises.extremenetworks.extremeProduct.summitX450a-48t
.iso.org.dod.internet.private.enterprises.extremenetworks.extremeProduct.summitX450a-24tDC
.iso.org.dod.internet.private.enterprises.extremenetworks.extremeProduct.summitX450a-24xDC
.iso.org.dod.internet.private.enterprises.extremenetworks.extremeProduct.summitX450a-24x
.iso.org.dod.internet.private.enterprises.extremenetworks.extremeProduct.summitX450a-48tDC
.iso.org.dod.internet.private.enterprises.extremenetworks.extremeProduct.summitX250-24t
.iso.org.dod.internet.private.enterprises.extremenetworks.extremeProduct.summitX250-24p
.iso.org.dod.internet.private.enterprises.extremenetworks.extremeProduct.summitX250-24x
.iso.org.dod.internet.private.enterprises.extremenetworks.extremeProduct.summitX250-48t
.iso.org.dod.internet.private.enterprises.extremenetworks.extremeProduct.summitX250-48p

☑ Translate Display

sysOID: .iso.org.dod.internet.private.enterprises.extremenetworks.extremeProduct.bd8810

FIGURE 7-11 Discovery Configurator – Other Discovery Tab - Translate Display Option

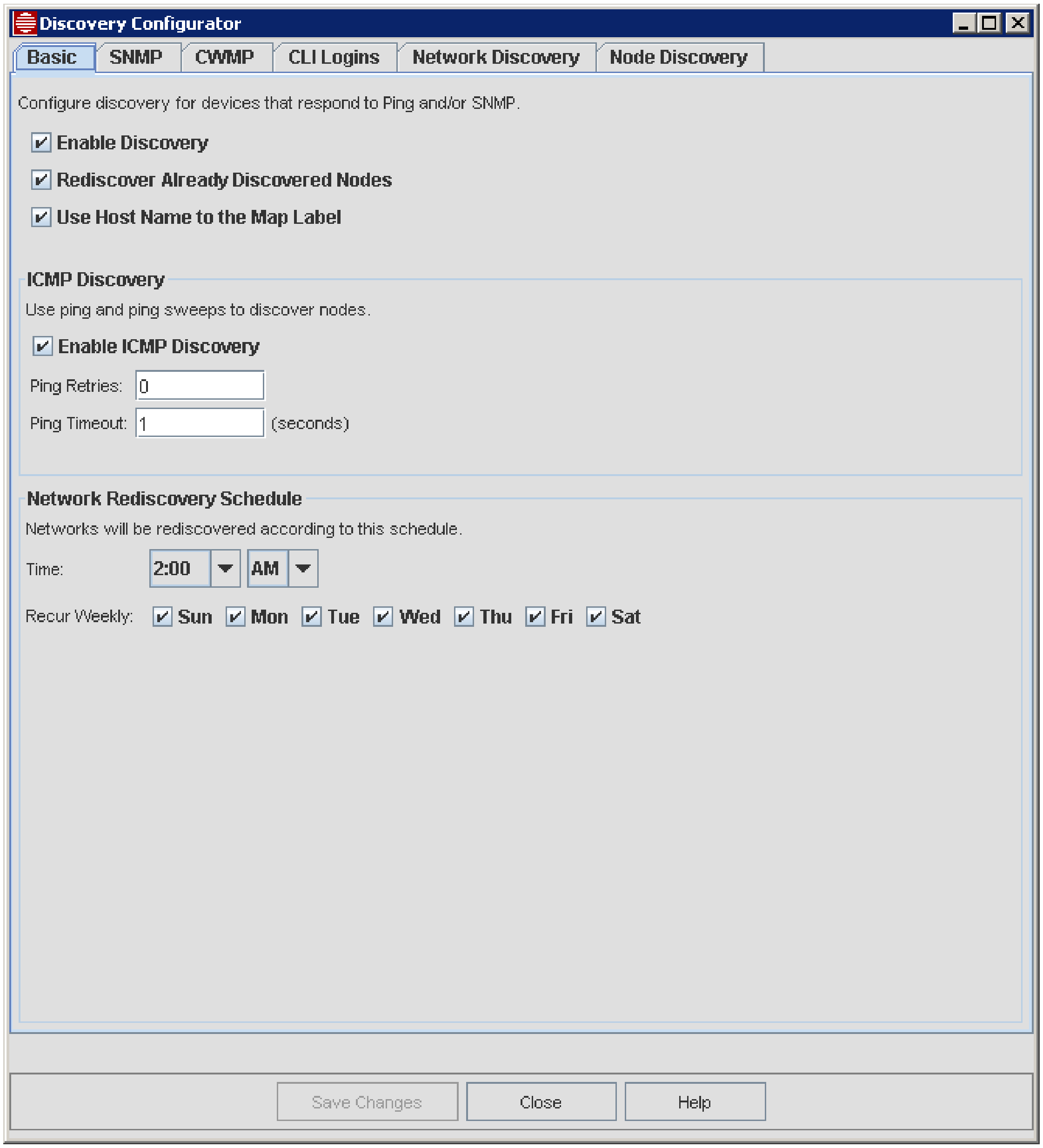
7.3 Discovery Configurator - Enterprise Edition

The Discovery Configurator has the following features:

1. The GUI allows enabling/disabling of Discovery.
2. ICMP Discovery (using Ping) can be configured, and SNMP Discovery is optional.
3. The local network can be discovered using a simple option.
4. Rediscovery can be disabled.
5. DHCP support is provided.
6. There is no sysOID filtering.

The Discovery Configurator includes six tabs: **Basic**, **SNMP**, **CWMP**, **CLI Logins**, **Network Discovery**, and **Node Discovery**. Each of these tabs is described below.

7.3.1 Basic Tab



Configure discovery for devices that respond to Ping and/or SNMP.

☑ Enable Discovery

☑ Rediscover Already Discovered Nodes

☑ Use Host Name to the Map Label

ICMP Discovery

Use ping and ping sweeps to discover nodes.

☑ Enable ICMP Discovery

Ping Retries: 0

Ping Timeout: 1 (seconds)

Network Rediscovery Schedule

Networks will be rediscovered according to this schedule.

Time: 2:00 AM

Recur Weekly: ☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

FIGURE 7-12 Discovery Configurator - Basic tab

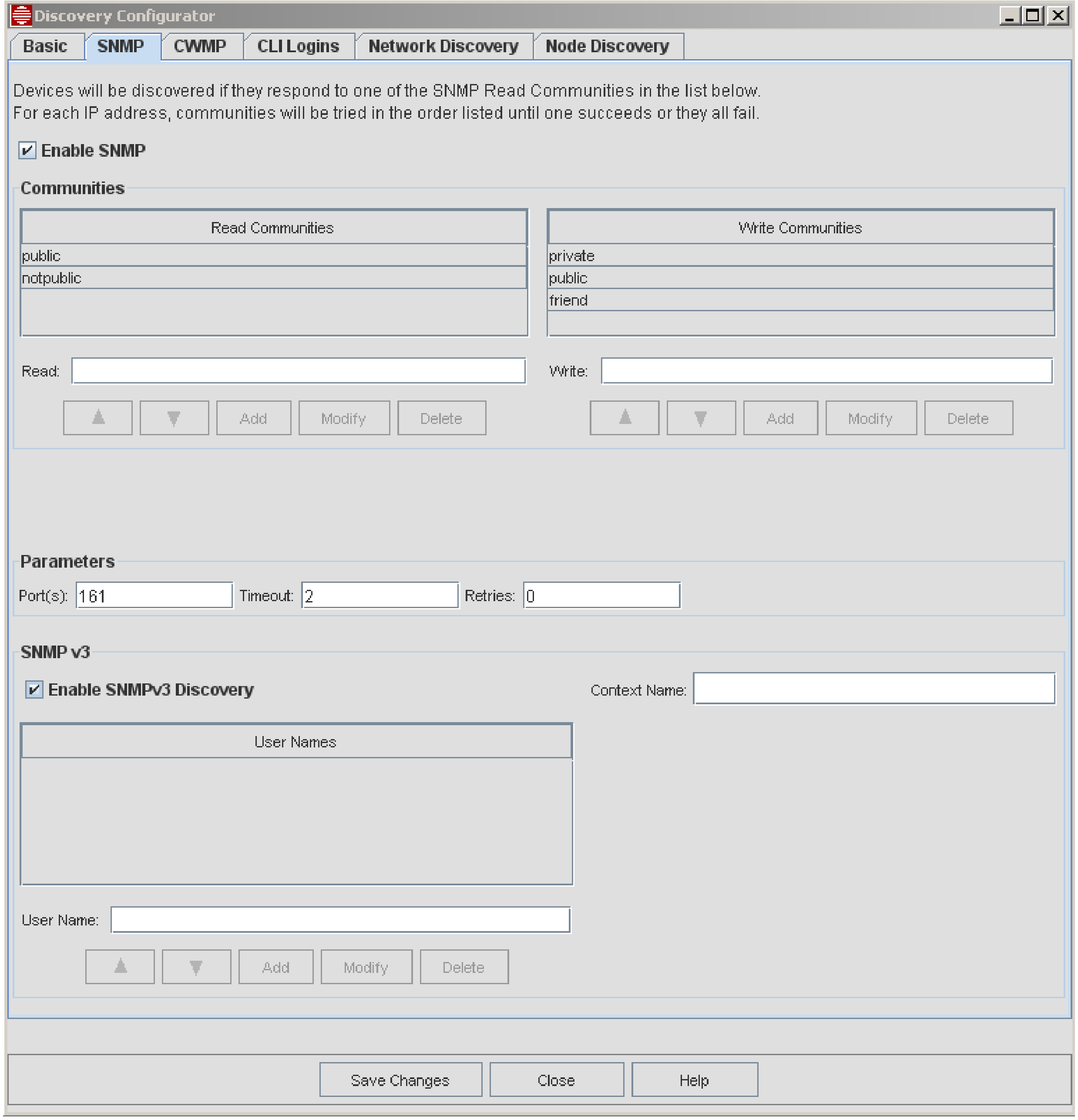
Options for the Basic tab are:

- **Enable Discovery** -The default is checked; if not checked, Discovery will not be performed.
- **Discover Local Network** - The default is not checked; if checked, nodes from the local network (where the NMS resides) are discovered.
- **Rediscover Already Discovered Nodes** - If checked (the default), nodes already discovered are rediscovered based on the rediscovery interval that has been set. If not checked, the node will not be rediscovered (and updates will not be detected).
- **Enable ICMP Discovery** - If checked (not the default), ICMP Ping is used for discovery.
    - **Ping Retries** - Number of times an ICMP Ping will be resent.

  - **Ping Timeout** - Number of seconds the Configurator waits before assuming there will be no response.
- **Rediscovery Schedule** - Choose an hour and one or more days of the week. Nightly rediscovery is recommended (default), but any number (including none) can be selected. No more than once every 24 hours is allowed.

7.3.2 SNMP Tabs

Refer to the following figure.



Devices will be discovered if they respond to one of the SNMP Read Communities in the list below.
For each IP address, communities will be tried in the order listed until one succeeds or they all fail.

☑ Enable SNMP

Read Communities	Write Communities
public	private
notpublic	public
	friend

Port(s): 161 Timeout: 2 Retries: 0

☑ Enable SNMPv3 Discovery

FIGURE 7-13 SNMP - EE Version

SNMP discovery can be enabled or disabled. If disabled, the rest of this tab is grayed-out. If enabled, the NMS will use this configuration during network discovery to test IP addresses for the presence of SNMP-enabled devices. Devices that respond will be added to the NMS database and will be monitored for status polling by periodically polling selected system variables (such as sysDescr).

The NMS performs “SNMP Ping” operations with each of the given read communities until a device responds or all communities have been tried and failed. (SNMP Pings are essentially SNMP get requests for selected system variables. Devices that respond are considered “connected” and those that don't are considered “unreachable”)

7.3.2.1 SNMPv2

For most devices, only read communities are used during discovery. Some devices, including iMG/RGs, require discovering write communities as well.

Communities will be attempted in the order displayed. The order may be modified by selecting a row and then clicking on the up/down buttons.

Communities may be added, modified, or deleted with the **Add**, **Modify** or **Delete** Buttons. The Add button will add to the list whatever is in the Read or Write text field. The Modify button will replace whatever is in the selected row with whatever has been typed in the Read or Write text field.

The SNMP agent port, timeout, and retry count can be configured as well. The defaults are 161, 10, and 0 respectively. Whereas 161 is the most commonly used SNMP agent port, others can be added as a space-separated list. Each port will be tried in the given order.

7.3.2.2 SNMPv3

There is the option enable SNMPv3 Discovery, which adds security and administration features. (For information on the relationships between the SNMP versions refer to RFC 3416.)

The SNMP panel allows the addition of Users following the User-based security model defined in RFC 3414. As RFC 3416, states, it is up to the only those principals (users) having legitimate rights can access or modify the values of any MIB objects supported by that entity.

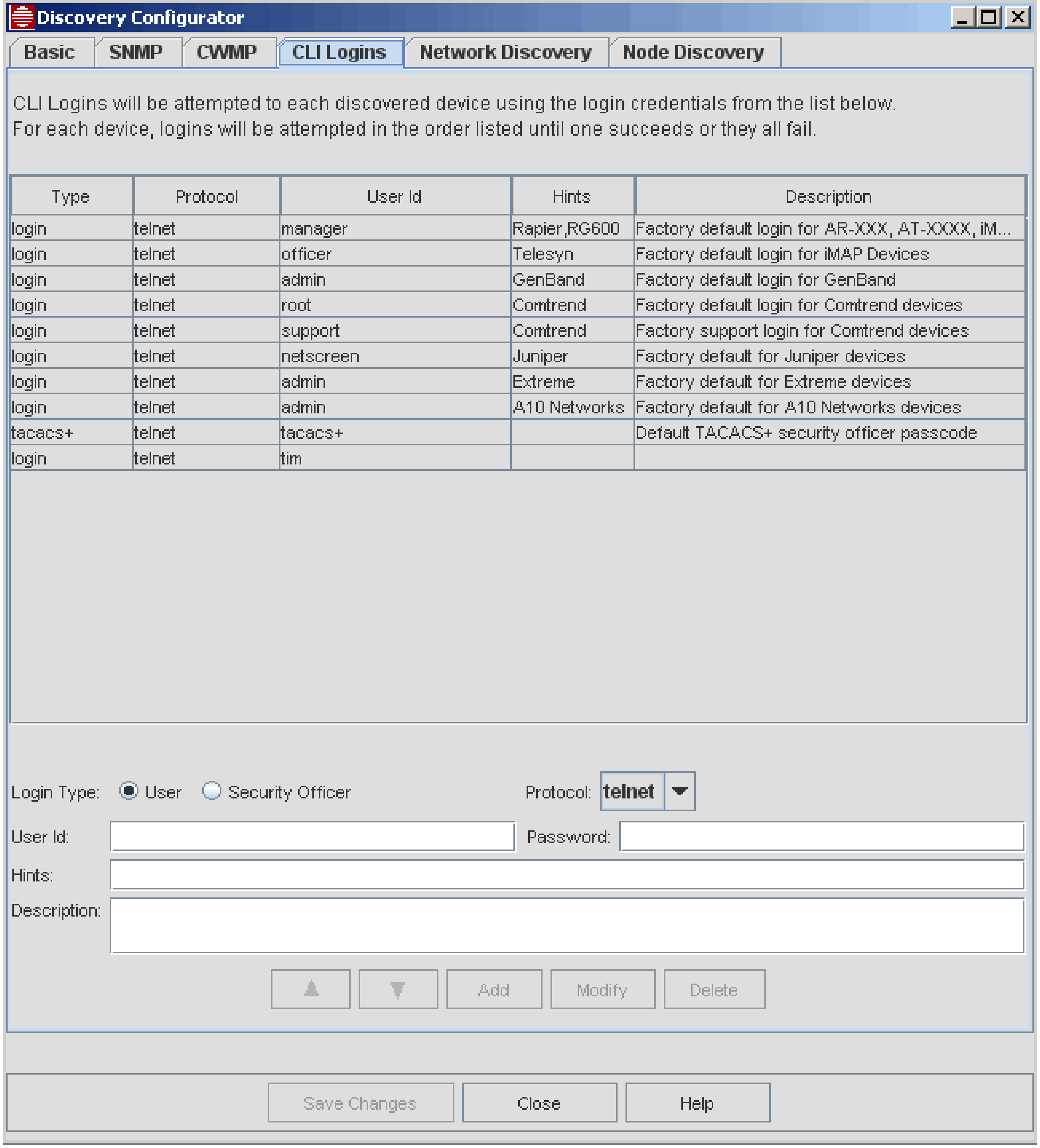
The SNMP panel includes the Enable SNMPv3 Discovery option, as shown in Figure 7-14. User Names are added by typing in the User Name field, the Context Field, and then selecting **Add**. Names can continue to be added and the order changed using the direction arrows. A name can be modified by selecting a name, changing the name in the User name field, and selecting **Modify**. Selecting Save Changes writes the values to the NMS

7.3.3 CWMP Tab

The CWMP (Common WAN management Protocol) Discovery tab is added for TR-69 Support. This tab allows setting the ACS (auto configuration server) login credentials on the NMS and creating a list TR-69 connection request login credentials for iMGs.

7.3.4 CLI Logins Tab

Refer to the following figure.



CLI Logins will be attempted to each discovered device using the login credentials from the list below.
For each device, logins will be attempted in the order listed until one succeeds or they all fail.

Type	Protocol	User Id	Hints	Description
login	telnet	manager	Rapier,RG600	Factory default login for AR-XXX, AT-XXXX, iM...
login	telnet	officer	Telesyn	Factory default login for iMAP Devices
login	telnet	admin	GenBand	Factory default login for GenBand
login	telnet	root	Comtrend	Factory default login for Comtrend devices
login	telnet	support	Comtrend	Factory support login for Comtrend devices
login	telnet	netscreen	Juniper	Factory default for Juniper devices
login	telnet	admin	Extreme	Factory default for Extreme devices
login	telnet	admin	A10 Networks	Factory default for A10 Networks devices
tacacs+	telnet	tacacs+		Default TACACS+ security officer passcode
login	telnet	tim		

Login Type: ● User ○ Security Officer Protocol: telnet

User Id: Password:

Hints:

Description:

FIGURE 7-14 CLI Logins Tab - EE Version

Status polling via ICMP or SNMP does not require CLI access; CLI discovery is only required when device configuration (backups, port management, VLAN management, etc.) is desired and is only applicable to fully-supported devices (refer to Section 1).

Once a device has been discovered by way of SNMP, more detailed discovery requiring a CLI login is required to manage the device. The NMS will attempt to log into each device until it either discovers an accepted login or all login attempts are rejected. The login sequence generally follows the order of the logins in the table. The order may be modified by selecting a row and then clicking on the up or down (▲▼) buttons.

The login sequence can be overridden by the Hints field. Hints are a comma-separated list of device category, sysLocation, IP address, and subnets (in x.x.x.x/bits notation). Login parameters for a device that matches any of the hints will be attempted before any other login parameters. If there are more than 1 login entry with matching hints, they will be attempted in the sequence from the list.

If all login attempts with matching hints fail, all of the entries without hints will be attempted until one is accepted or all are rejected. And if all of those fail, all of the rest (without matching hints) will be attempted.

The Description field is a free format reminder of what each login entry represents.

There are 2 login types: User and Security Officer, which are specified by the radio button. The “user” type uses the User Id and Password to initially log into the device. User login is all that's required for iMAPs running without TACPLUS.

If a device is running with TACPLUS enabled, the NMS also needs a Security Officer passcode (to enable securityofficer). Security Officer passcodes can be designated by clicking on the Security Officer radio button. For Security Officer, the User Id field is not applicable and will be disabled and set to “tacacs+”. (You can still define a user login with the user id tacacs+, if necessary, by clicking on the User radio button instead of the Security Officer radio button) Security Officer passcodes will be attempted as ordered in the list and as overridden by Hints. Since multiple Security Officer passcodes are permissible, be sure to use the description field to keep track of which is which (since they will typically be indistinguishable without displaying the passcode).

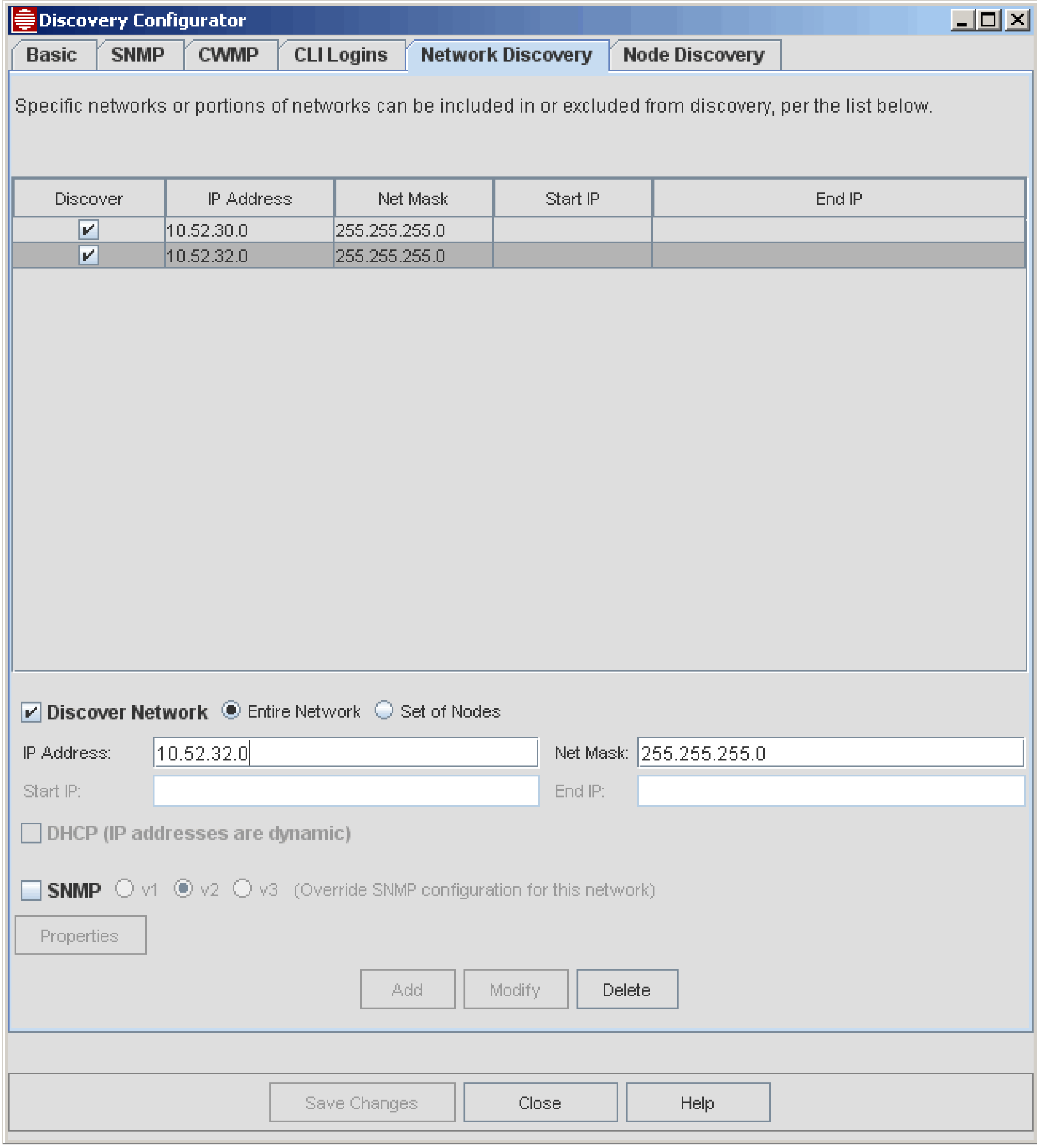
There is also the option to select the protocol. The default is telnet, but here is also the option to choose SSH. These are also added to the User ID list.

Most Allied Telesis devices support SSHv2. Using SSH involves configuring and enabling the SSH server. This involves:

- Server authentication, confidentiality, and integrity
- User authentication through the use of a password and/or public key
- Connection encryption for interactive login sessions

Refer to customer documents for Allied Telesis products for support of specific SSH features.

7.3.5 Network Discovery Tab



Specific networks or portions of networks can be included in or excluded from discovery, per the list below.

Discover	IP Address	Net Mask	Start IP	End IP
☑	10.52.30.0	255.255.255.0		
☑	10.52.32.0	255.255.255.0		

☑ Discover Network ● Entire Network ○ Set of Nodes

IP Address: 10.52.32.0 Net Mask: 255.255.255.0

Start IP: End IP:

□ DHCP (IP addresses are dynamic)

□ SNMP ○ v1 ● v2 ○ v3 (Override SNMP configuration for this network)

FIGURE 7-15 Network Discovery Tab - EE Version

This tab specifies networks to discover (or exclude from discovery). The discovery process will attempt to discover devices at all IP addresses in the network (or exclude all such addresses if configured for exclusion).

Networks can be added, modified, or deleted with the **Add**, **Modify**, and **Delete** buttons.

The “Discover Network” toggle, when checked, means to discover the network (or subnet). When unchecked, that network (or subnet) will be ignored during discovery.

The “Entire Network” radio button, when selected, means to use all addresses in the network, specified by the IP Address and Net Mask fields. When “Set of Nodes” is selected instead, only the addresses from the Start IP to the End IP will be discovered.

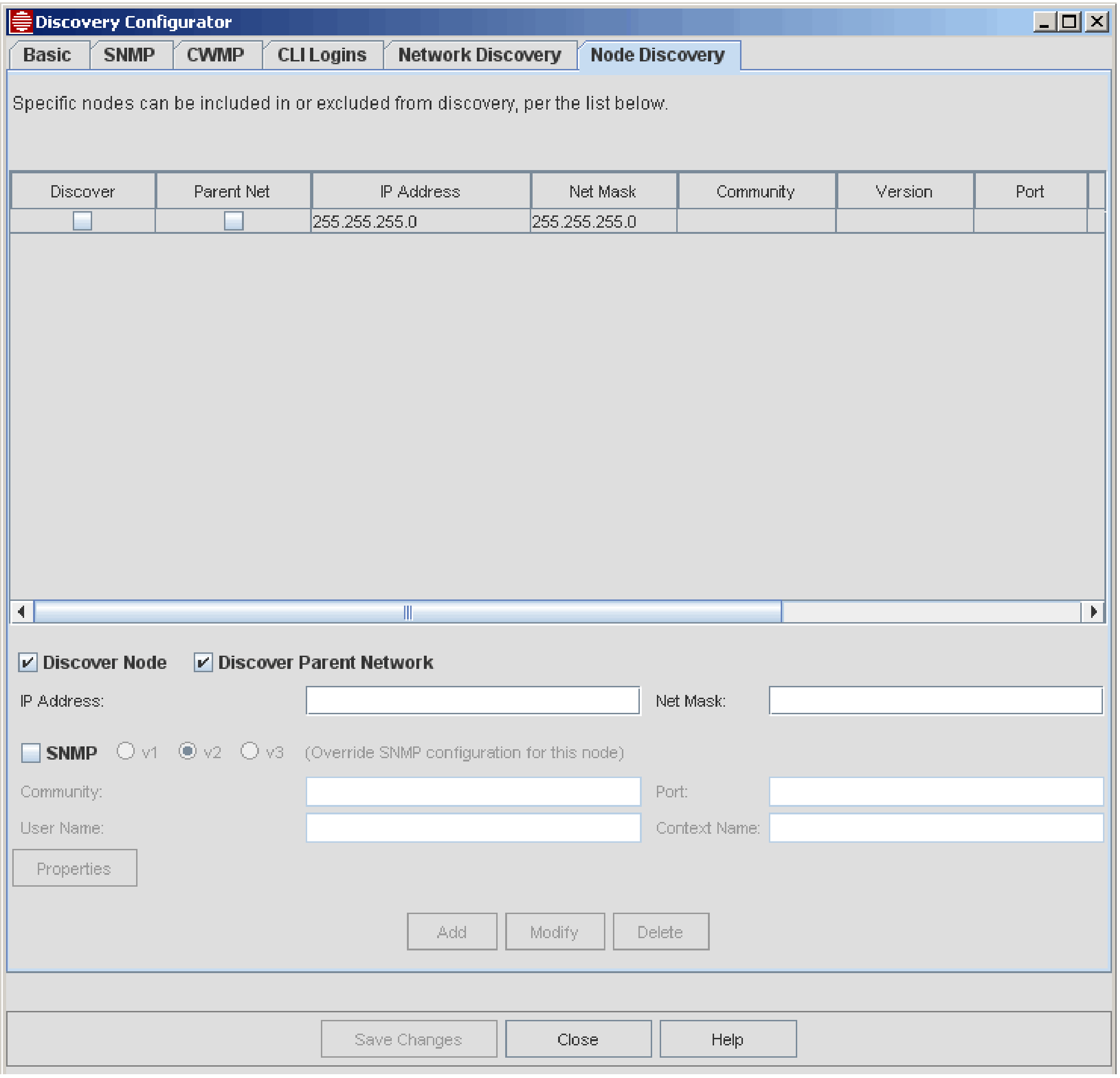
When “Set of Nodes” is selected, the DHCP option becomes available. Use this option if IP addresses are assigned dynamically. The NMS will then use MAC addresses to identify hosts rather than IP addresses or host names.

If SNMP discovery is enabled, network discovery will normally use the parameters configured on the SNMP tab, but they can be overridden for specific networks and subnets by selecting the SNMP option on this tab.The properties to fill in depend on the SNMP version selected.

A version of SNMP can be chosen to override what is configured for the network. After choosing the SNMP version, selecting the **Properties** button allows the parameters to be filled in.

Caution: It is not possible to delete a network from discovery once discovery begins on that network. Discovery begins any time immediately after saving changes. Therefore, to permanently remove a network from the discovery configuration, shut down the NMS to shut down the discovery process and use the standalone Discovery Configurator to delete the unwanted network. Networks are successfully deleted, however, when deleted before saving changes.

7.3.6 Node Discovery Tab



Specific nodes can be included in or excluded from discovery, per the list below.

Discover	Parent Net	IP Address	Net Mask	Community	Version	Port
□	□	255.255.255.0	255.255.255.0			

☑ Discover Node ☑ Discover Parent Network

□ SNMP ○ v1 ● v2 ○ v3 (Override SNMP configuration for this node)

FIGURE 7-16 Node Discovery Tab - EE Version

This tab specifies specific nodes to discover (or exclude from discovery).

Nodes can be added, modified, or deleted with the **Add**, **Modify**, and **Delete** buttons.

The “Discover Node” toggle, when checked, means to discover the node. When unchecked, that node will be ignored (excluded) from discovery.

The “Discover Parent Network” tab means to discover all the devices in the parent network as well. The parent network will be considered to be all IP addresses in the same subnet as the node defined by its IP Address and its Net Mask. When unchecked, only the one node will be discovered.

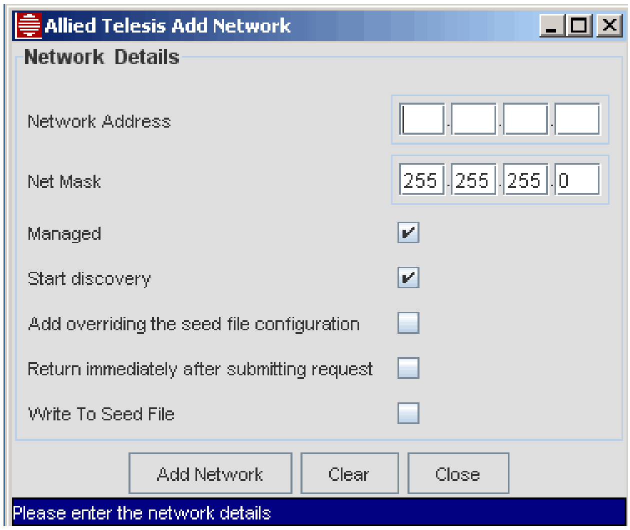
If SNMP discovery is enabled, node discovery will normally use the parameters configured on the SNMP tab, but they can be overridden for specific nodes by selecting the SNMP option on this tab and supplying the version, community, and port values.

The SNMP version used can be selected here as well, with the properties determined by the version.

Note: If nodes are failing initial discovery, you can (for SNMP) change the “Retries” parameter (default 0) and the “Timeout” parameter from the SNMP v1/v2c Tab, and then use the ***Network Inventory / Edit -> Add Node*** *to retry initial discovery. If you are using ICMP, you can change the “Retries” parameter (default 0) and the Timeout parameter from the Basic Tab.*

7.4 Adding a Network or Node from the Network Inventory

You can add an individual network or node immediately by selecting the Network Inventory node in the Network Objects tree. To add a new network go to **Edit > Add Network**. To add a new node go to **Edit > Add Node**. This brings up the Allied Telesis Add Network or Add Node panel, respectively, as shown below.



Allied Telesis Add Network

Network Details

Network Address [ ].[ ].[ ].[ ]

Net Mask 255.255.255.0

Managed ☑

Start discovery ☑

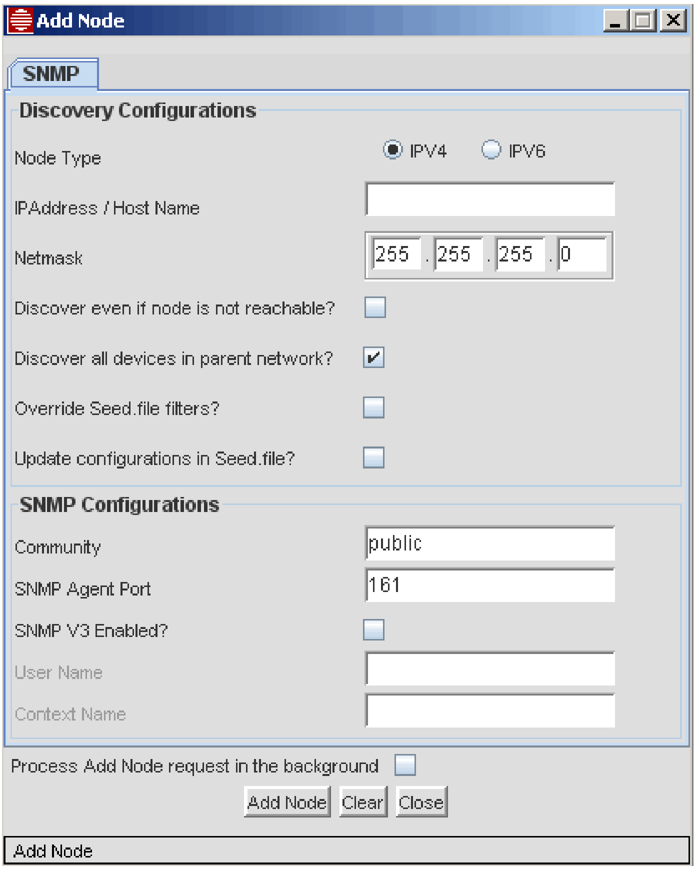
Add overriding the seed file configuration □

Return immediately after submitting request □

Write To Seed File □

Please enter the network details

FIGURE 7-17 Add Network (From Network Inventory)



Discovery Configurations

Node Type ● IPV4 ○ IPV6

IPAddress / Host Name

Netmask 255 . 255 . 255 . 0

Discover even if node is not reachable? □

Discover all devices in parent network? ☑

Override Seed.file filters? □

Update configurations in Seed.file? □

SNMP Configurations

Community public

SNMP Agent Port 161

SNMP V3 Enabled? □

User Name

Context Name

Process Add Node request in the background □

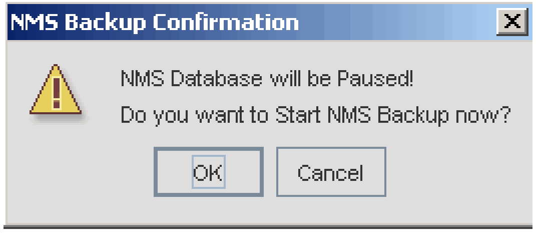
Add Node

FIGURE 7-18 Add Node (From Network Inventory)

7.5 Backup and Restore

7.5.1 AlliedView NMS Backup (On Demand)

To make an immediate backup of the server and database files, choose from the main menu *Tools -> NMS Database Backup*, and the option *On Demand*. A dialog box appears, as shown in Figure 7-19.

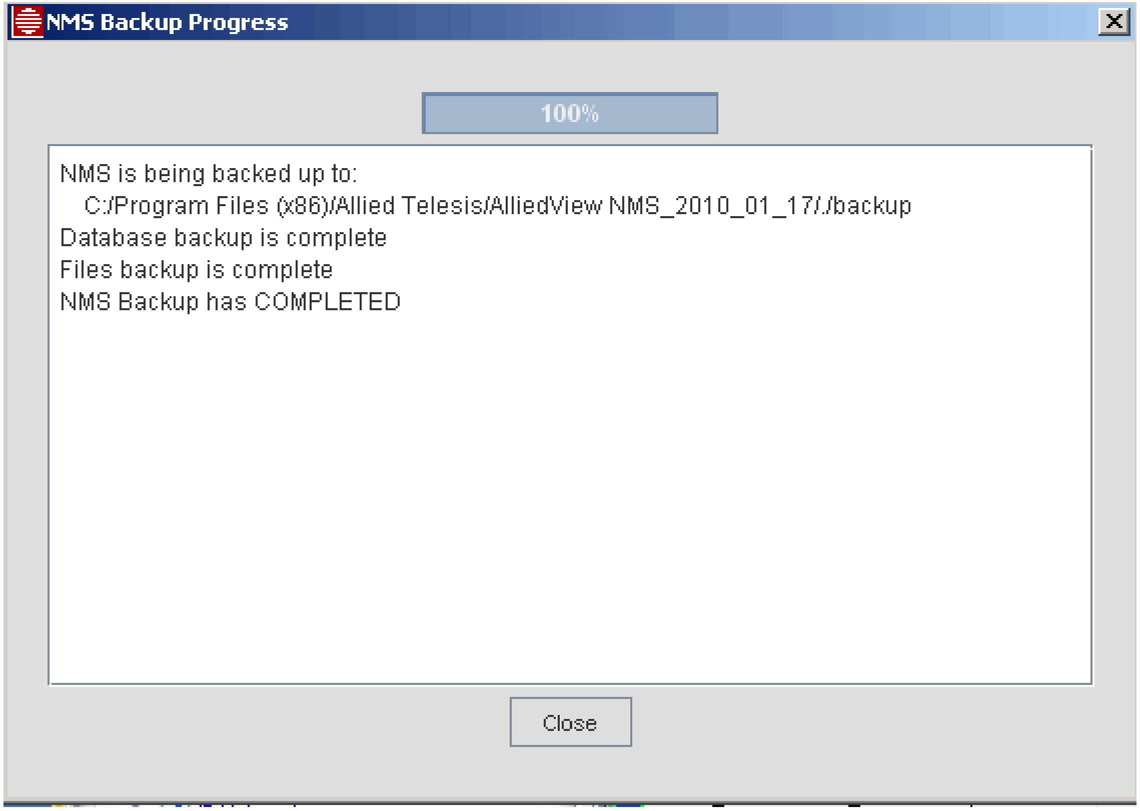


NMS Database will be Paused!

Do you want to Start NMS Backup now?

FIGURE 7-19 NMS Backup Confirmation Dialog

Clicking **OK** starts the backup process window. When finished, the window will show whether the backup was successful and where the backups were written to, as shown in Figure 7-20.



```
NMS is being backed up to:
   C:/Program Files (x86)/Allied Telesis/AlliedView NMS_2010_01_17/./backup
Database backup is complete
Files backup is complete
NMS Backup has COMPLETED
```

FIGURE 7-20 Backup Process Complete Window

The controlling of where the backup is written to is explained in "Configuring Backup Parameters for AlliedView NMS" on page 128.

7.5.2 AlliedView NMS Backup (Scheduled)

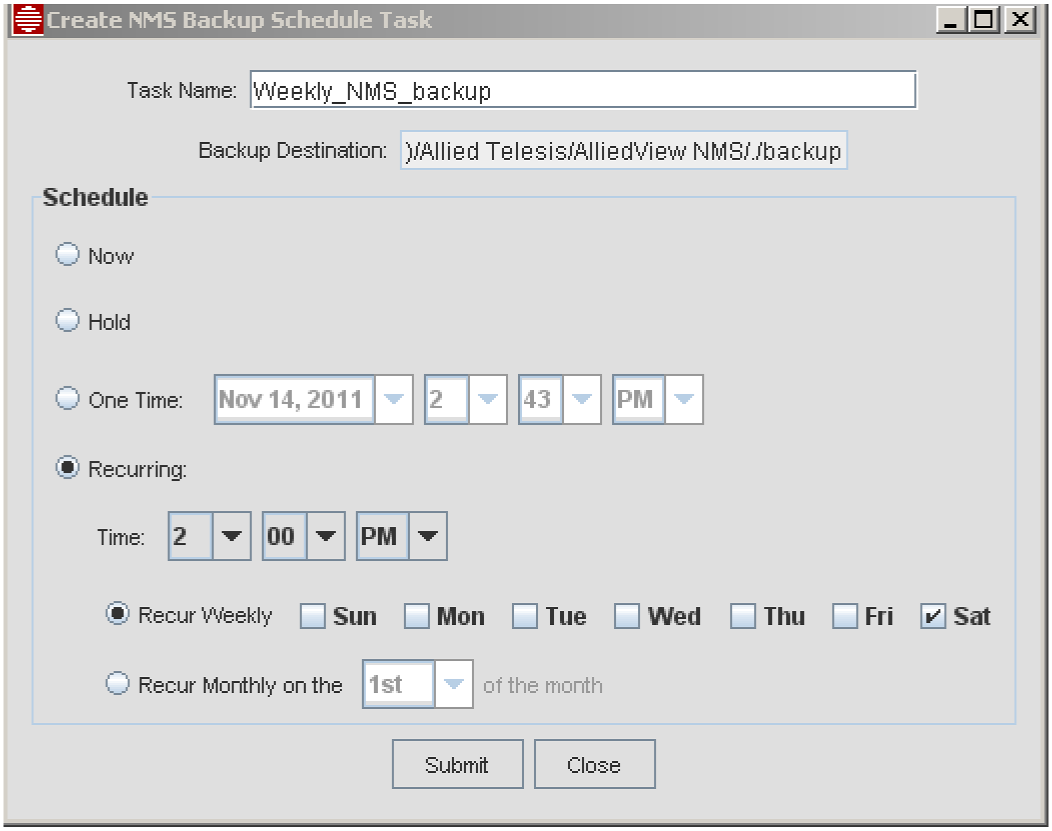
To backup the NMS server on a schedule, choose from the main menu *Tools -> NMS Database Backup*, and the option *Scheduled*. A dialog box appears, as shown in Figure 7-21.

The form has the following options:

- The **Task Name** is by default the time of the backup, but the user should give a descriptive name of the type of backup (such as NMS_weekly_backup).
- The **Backup Destination** is part of the restore process and are explained in "Configuring Backup Parameters for AlliedView NMS" on page 128.
- The **Schedule** panel has the following options:
  - **Now** is for a one-time only.
  - **Hold** is to create the task and give it a task name but not to attach a specific time or schedule.
  - **One Time** is to set a time in the future when the backup will be performed.
  - **Recurring** has further options for recurring at a specific time on a weekly or monthly basis.

Caution: It is highly recommended that the Backup Scheduler be used so that a recent snapshot of the NMS configuration may be available in case of server failure. (Backups can occur as often as once a day if desired.) Moreover, the backup should be written to a separately mounted disk. (Refer to "Configuring Backup Parameters for AlliedView NMS" on page 128.)

Clicking **Submit** brings up the **Task Details** window so that the task can be modified (if needed) and then added to other NMS tasks. (Clicking **Close** on the **Task Details** window will add the task to the tasklist. This user can then view the task by selecting *Tools* -> *View Tasks* and perform further actions. The tasklist is described in "Managing Tasks" on page 339.



Create NMS Backup Schedule Task

Task Name: Weekly_NMS_backup

Backup Destination:)/Allied Telesis/AlliedView NMS/./backup

Schedule

○ Now

○ Hold

○ One Time: Nov 14, 2011 2 43 PM

● Recurring:

Time: 2 00 PM

● Recur Weekly □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri ☑ Sat

○ Recur Monthly on the 1st of the month

FIGURE 7-21 NMS Backup Schedule

7.5.3 Configuring Backup Parameters for AlliedView NMS

A backup of the NMS configuration can be performed on demand or on a schedule. When the files are being backed up on demand, the console window shows the path where the files are being copied. When the files are being backed up on a schedule, the **Backup Destination** field (seen in Figure 7-21) shows this path.

The path used is controlled by the file:

`<NMS_Home>/conf/AT_NmsBackupFiles.conf`

This file includes the following parameters:

- `ATINMS_BACKUP_DEST`

  This where the NMS backups are stored. The default is `<NMS_Home>/backup`

- `ATIDEVICE_BACKUP_DEST`

  This is where device backups are stored. The default is `<NMS_Home>/backup`

- `ATIDEVICE_BACKUP_LIMIT`

  Refer to "Device Backup (Per-Device Limit)" on page 131.

Note: *In most cases, the user should change the directory path to one where you normally send backup files. The server should have sufficient space and be reliable for backup purposes.*

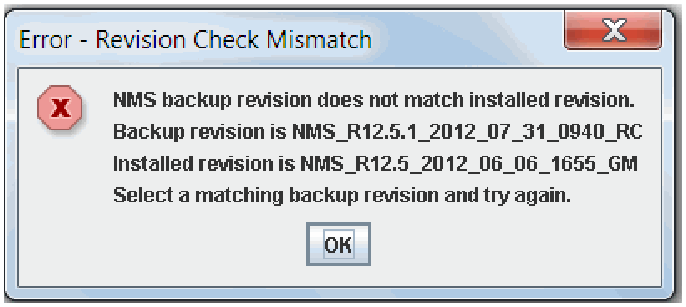
Note: Changes made to `AT_NmsBackupFiles.conf` *are enabled as soon as the file is changed, so a server restart is not needed.*

7.5.4 Restore the AlliedView NMS (GUI Screens)

There is a set of GUI screens to perform a restore.

Caution: A restore requires the server to be shut down and then restarted. If this feature is used while the AlliedView NMS is running, there is an error message. Moreover, any data changed since the last backup will be lost.

Caution: A restore should only be done on the same software version in which the backup was performed. If the software versions do not match, the following appears when starting the restore.



Error - Revision Check Mismatch

NMS backup revision does not match installed revision.
Backup revision is NMS_R12.5.1_2012_07_31_0940_RC
Installed revision is NMS_R12.5_2012_06_06_1655_GM
Select a matching backup revision and try again.

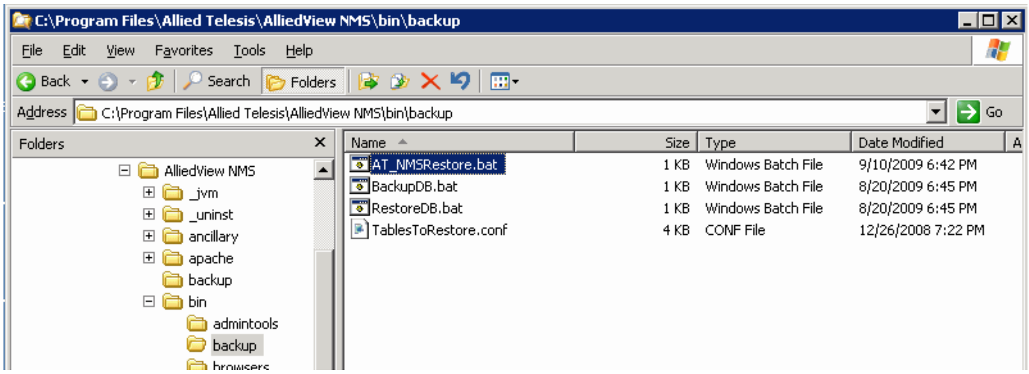
FIGURE 7-22 Warning for Software Version Mismatch for a Restore

1. Shut down the server (using the *Start -> Programs* menu path).
2. Start the tool:

   On Windows, from the bin/backup directory, select `AT_NMSRestore.bat`.

   On Linux, from the bin/backup directory, execute `./AT_NMSRestore.sh`

   Refer to the following figure for the Windows folder.



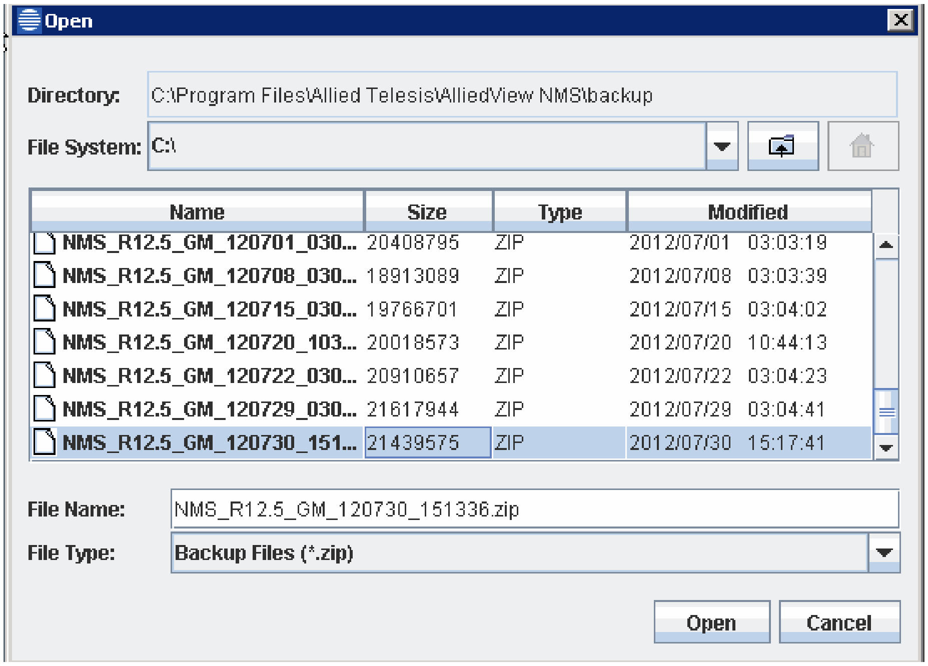
C:\Program Files\Allied Telesis\AlliedView NMS\bin\backup

Address C:\Program Files\Allied Telesis\AlliedView NMS\bin\backup

Name	Size	Type	Date Modified
AT_NMSRestore.bat	1 KB	Windows Batch File	9/10/2009 6:42 PM
BackupDB.bat	1 KB	Windows Batch File	8/20/2009 6:45 PM
RestoreDB.bat	1 KB	Windows Batch File	8/20/2009 6:45 PM
TablesToRestore.conf	4 KB	CONF File	12/26/2008 7:22 PM

FIGURE 7-23 Starting the NMS Recovery Feature (Windows)

3. Selecting the NMS exec file brings up the Restore Tool. Use the **Browse** button to bring up the relevant backup file. In searching there is the Zip option to search through only zip type files. Refer to the following figure.



Directory: C:\Program Files\Allied Telesis\AlliedView NMS\backup

File System: C:\

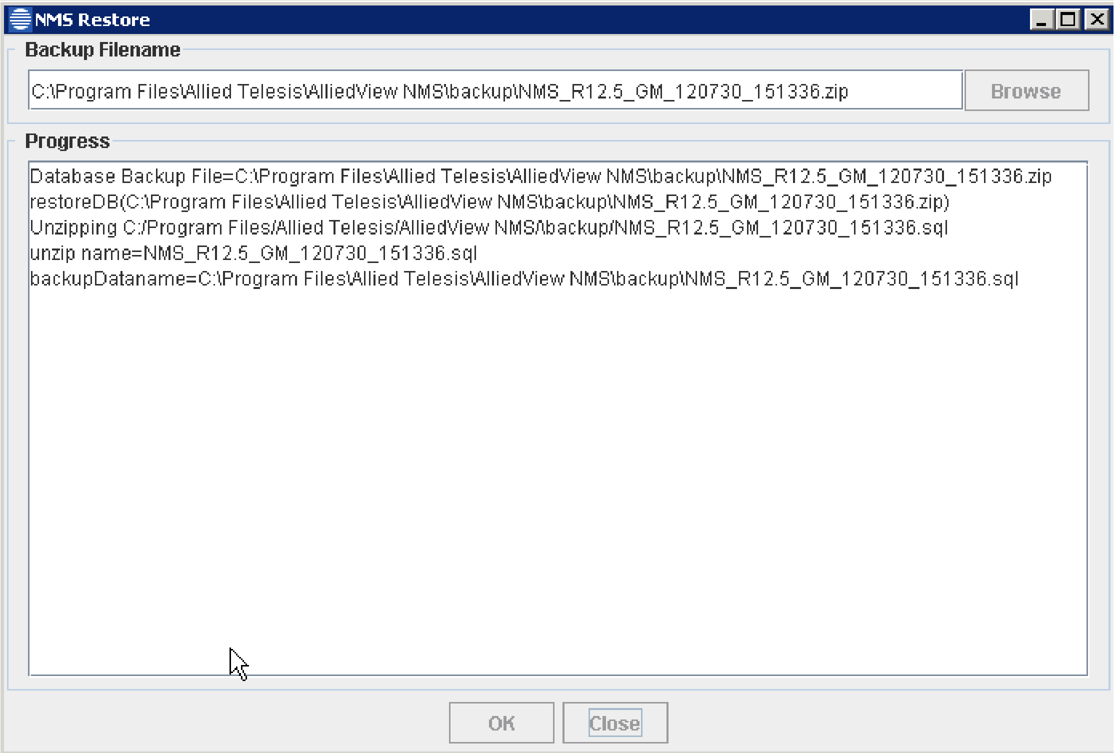
Name	Size	Type	Modified
NMS_R12.5_GM_120701_030...	20408795	ZIP	2012/07/01 03:03:19
NMS_R12.5_GM_120708_030...	18913089	ZIP	2012/07/08 03:03:39
NMS_R12.5_GM_120715_030...	19766701	ZIP	2012/07/15 03:04:02
NMS_R12.5_GM_120720_103...	20018573	ZIP	2012/07/20 10:44:13
NMS_R12.5_GM_120722_030...	20910657	ZIP	2012/07/22 03:04:23
NMS_R12.5_GM_120729_030...	21617944	ZIP	2012/07/29 03:04:41
NMS_R12.5_GM_120730_151...	21439575	ZIP	2012/07/30 15:17:41

File Name: NMS_R12.5_GM_120730_151336.zip

File Type: Backup Files (*.zip)

FIGURE 7-24 Selecting Files for AlliedView Restore

4. Press **Open** to bring up the NMS Restore window with the selected backup file, and then **OK** to start the restore. Progress and error messages are displayed in the Progress window during the restoration process and saved to a log file in the backup directory (this is not the bin/backup directory from where the GUI is launched). Refer to the following figures.



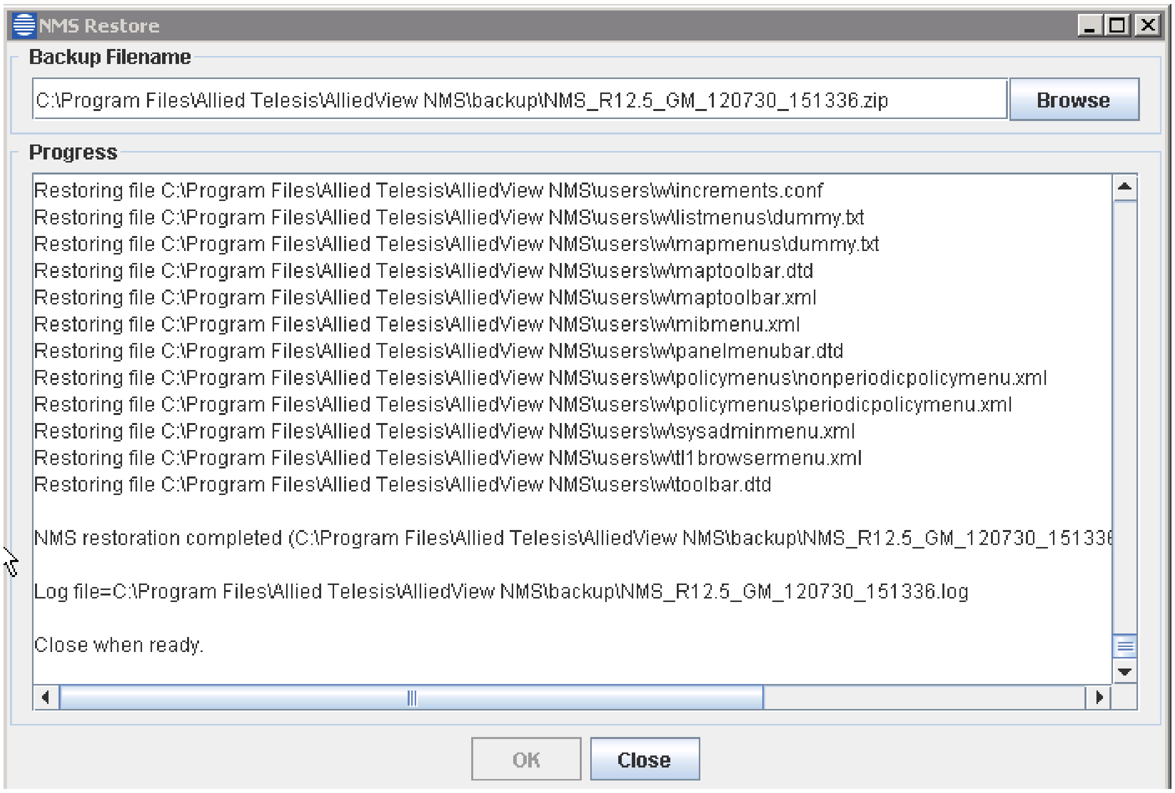
Backup Filename

C:\Program Files\Allied Telesis\AlliedView NMS\backup\NMS_R12.5_GM_120730_151336.zip

Progress

```
Database Backup File=C:\Program Files\Allied Telesis\AlliedView NMS\backup\NMS_R12.5_GM_120730_151336.zip
restoreDB(C:\Program Files\Allied Telesis\AlliedView NMS\backup\NMS_R12.5_GM_120730_151336.zip)
Unzipping C:/Program Files/Allied Telesis/AlliedView NMS/backup/NMS_R12.5_GM_120730_151336.sql
unzip name=NMS_R12.5_GM_120730_151336.sql
backupDataname=C:\Program Files\Allied Telesis\AlliedView NMS\backup\NMS_R12.5_GM_120730_151336.sql
```

FIGURE 7-25 AlliedView NMS Restore - Start



C:\Program Files\Allied Telesis\AlliedView NMS\backup\NMS_R12.5_GM_120730_151336.zip

```
Restoring file C:\Program Files\Allied Telesis\AlliedView NMS\users\w\increments.conf
Restoring file C:\Program Files\Allied Telesis\AlliedView NMS\users\w\listmenus\dummy.txt
Restoring file C:\Program Files\Allied Telesis\AlliedView NMS\users\w\mapmenus\dummy.txt
Restoring file C:\Program Files\Allied Telesis\AlliedView NMS\users\w\maptoolbar.dtd
Restoring file C:\Program Files\Allied Telesis\AlliedView NMS\users\w\maptoolbar.xml
Restoring file C:\Program Files\Allied Telesis\AlliedView NMS\users\w\mibmenu.xml
Restoring file C:\Program Files\Allied Telesis\AlliedView NMS\users\w\panelmenubar.dtd
Restoring file C:\Program Files\Allied Telesis\AlliedView NMS\users\w\policymenus\nonperiodicpolicymenu.xml
Restoring file C:\Program Files\Allied Telesis\AlliedView NMS\users\w\policymenus\periodicpolicymenu.xml
Restoring file C:\Program Files\Allied Telesis\AlliedView NMS\users\w\sysadminmenu.xml
Restoring file C:\Program Files\Allied Telesis\AlliedView NMS\users\w\tl1browsermenu.xml
Restoring file C:\Program Files\Allied Telesis\AlliedView NMS\users\w\toolbar.dtd

NMS restoration completed (C:\Program Files\Allied Telesis\AlliedView NMS\backup\NMS_R12.5_GM_120730_15133

Log file=C:\Program Files\Allied Telesis\AlliedView NMS\backup\NMS_R12.5_GM_120730_151336.log

Close when ready.
```

FIGURE 7-26 AlliedView NMS Restore - Finish

7.5.5 Device Backup (Per-Device Limit)

Daily backups of a large network will eventually use up all the disk memory unless customers manually purge old files. One feature to address this is using file configuration as follows:

The limit is configured in `conf/AT_NmsBackupFiles.conf`

The property is `ATIDEVICE_BACKUP_LIMIT`

Setting this to zero is equivalent to no limit.

Setting this to a non-zero number is the number of device backups allowed. For example, if you set the limit to 100, and have backups scheduled to occur daily for all devices, the AlliedView NMS will keep the most recent 100 days of backups for each device.

In another example with the limit set to 100, if you have one device with backups twice daily, the AlliedView NMS would keep the most recent 50 days for that specific device.

Note: There is a Purge Files button that is added to the MDTI application. Refer to "Backup/Restore (with Purge Button)" on page 279.

7.6 Inventory Reporting

Inventory reporting is a utility that can help you troubleshoot network-wide problems that may be related to hardware characteristics such as card revisions, serial numbers, or engineering change orders. Inventory reporting is available for:

- iMAP devices running software release 15.x.x and above
- Layer 2/3 switches running AlliedWare Plus (AW+) software release 5.x.x or above

- All iMG devices

If an iMAP device is running AlliedWareNSP release 6.18.x.x or above or a layer 2/3 switch is running AW+ release 5.4.4 or above, you can use inventory reporting to obtain the CFC base MAC addresses (iMAP) or MAC addresses used for licensing (AW+) that are required for release activation licenses.

You can view data for all devices in the network or just a subset of devices for troubleshooting purposes.

The data is presented in spreadsheet format. Table 7-2 lists the AW+ system data included in the Layer 2/3 Switch Report. Table 7-3 lists the iMAP system and card data included in the iMAP Card Report. Table 7-4 lists the system data included in the iMG Unit Report.

TABLE 7-2 Layer 2/3 Switch Report

System
Device
Stack member
Board
Bay
Board Name
Rev
Serial number
Software version
License MAC

TABLE 7-3 iMAP Card Report

System	Card
Device	Device
Description	Slot
Shelf Serial Number	Type
Shelf CLEI Code	State
Shelf MAC	Model Number (Revision)
Hostname	Serial Number
Location	CLEI Code
Name	Engineering Change Order
Engineering Change Order	Deviation(s)
Deviation(s)	Base MAC Address (available for cards running AlliedWareNSP release 6.18.x.x and above)
	Running Load
	Preferred Load
	Temporary Load

TABLE 7-4 iMG Unit Report

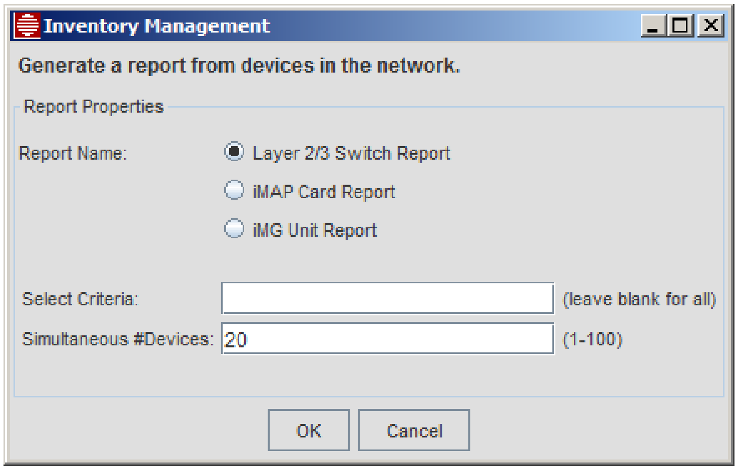
System
IP
Customer
Location
Type
Rev
Serial Number
Software Version
Recovery Version

You must have an application that reads comma-separated values (CSV) files installed on the NMS client machine to view the spreadsheet correctly. Once the data is in the spreadsheet you can save it to a file for future use.

7.6.1 Producing an Inventory Report

To produce an inventory report:

1. From the **Tools** menu, go to **Inventory Report Utility**. The **Inventory Management** box appears.



Inventory Management

Generate a report from devices in the network.

Report Properties

Report Name: ● Layer 2/3 Switch Report ○ iMAP Card Report ○ iMG Unit Report

Select Criteria: (leave blank for all)

Simultaneous #Devices: 20 (1-100)

FIGURE 7-27 Inventory Management

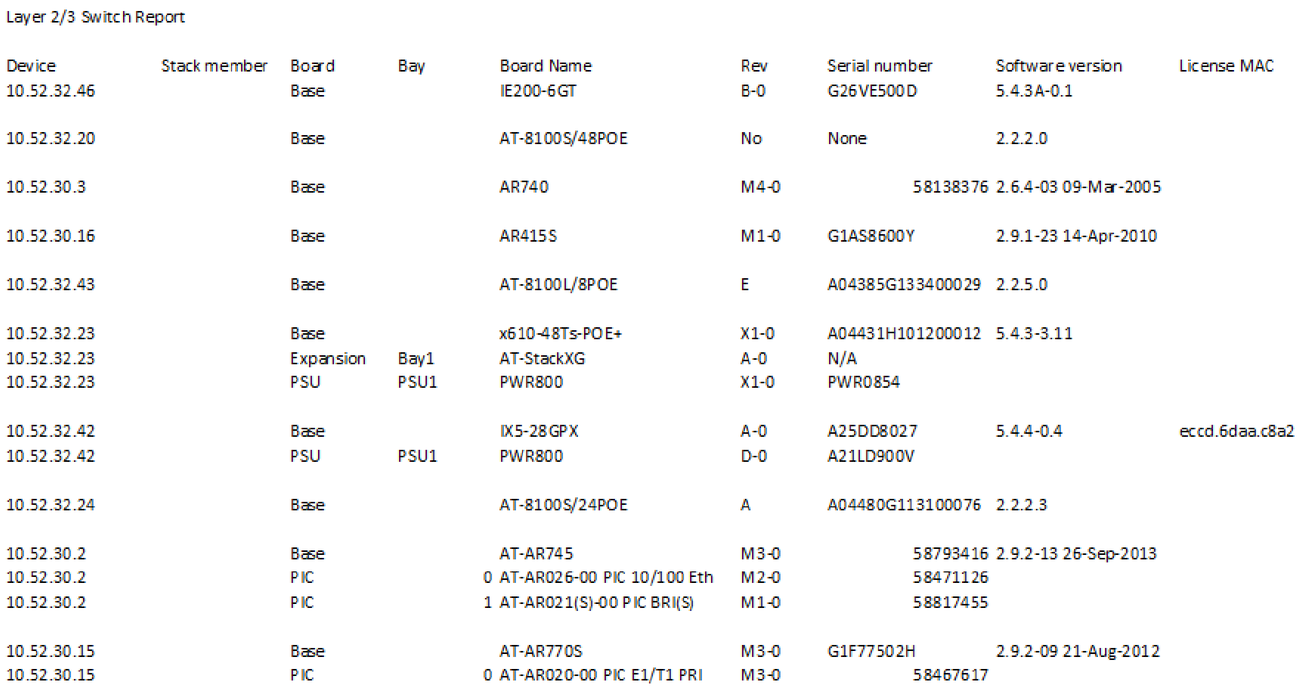
2. For **Report Name**, select the type of report you want to run. This is the name of the report.
3. In the **Select Criteria** field, do one of the following:
   - Leave it blank to generate a report for all devices in the network.
   - Enter a comma-separated list of match criteria for a subset of devices. You can use hostname, sysLocation, IP or subnet.
     - For hostname and sysLocation you can use partial names.
     - The IP address must be exact.
     - A subnet must be in the format X.X.X.X/XX.
4. In the **Simultaneous #Devices** field, enter the maximum number of devices to query concurrently. You can query up to 100 devices at a time. Querying multiple devices simultaneously speeds up report generation but can impact network performance.
5. Click **OK** to generate the report.

While the report is generating a progress box appears. Clicking **Cancel** interrupts report generation and the report opens with what has been generated so far.

Figure 7-28 is an example of a Layer 2/3 Switch Report.

Figure 7-29 is a partial example of an iMAP Card Report. The example does not include all of the columns that appear in the report.

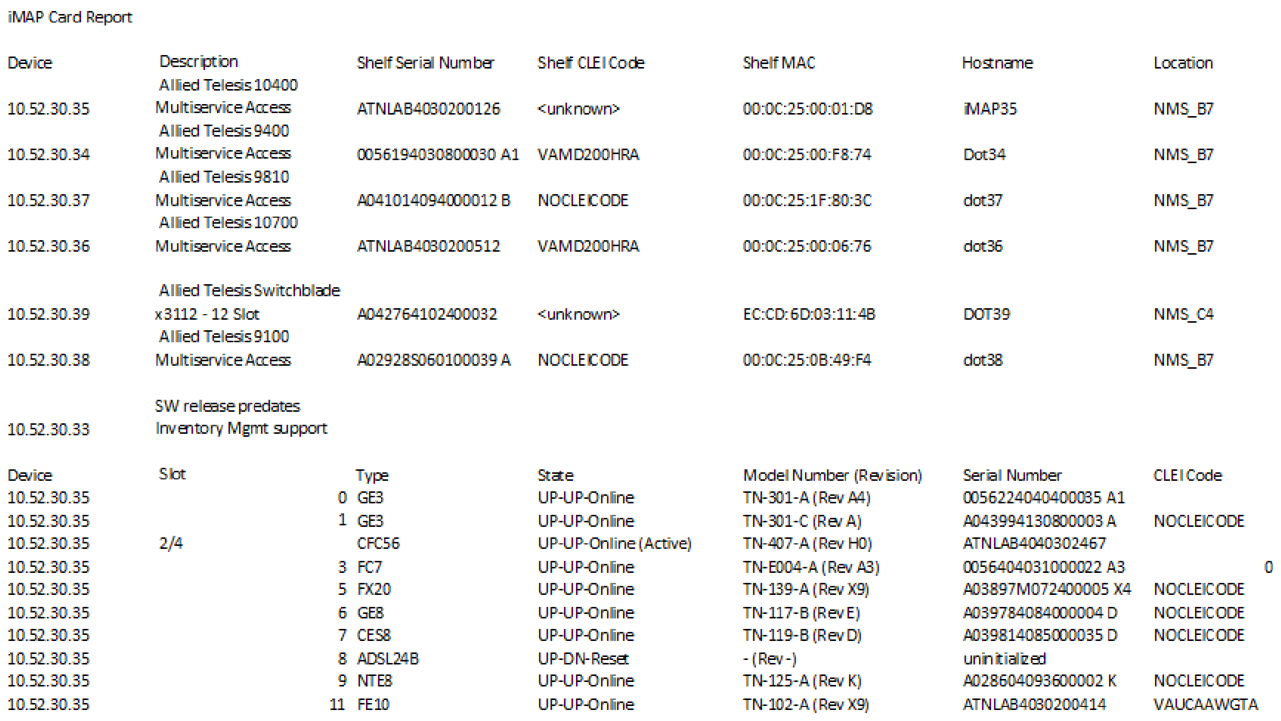
Figure 7-30 is an example of an iMG Unit Report.



Layer 2/3 Switch Report

Device	Stack member	Board	Bay	Board Name	Rev	Serial number	Software version	License MAC
10.52.32.46		Base		IE200-6GT	B-0	G26VE500D	5.4.3A-0.1	
10.52.32.20		Base		AT-8100S/48POE	No	None	2.2.2.0	
10.52.30.3		Base		AR740	M4-0	58138376	2.6.4-03 09-Mar-2005	
10.52.30.16		Base		AR415S	M1-0	G1AS8600Y	2.9.1-23 14-Apr-2010	
10.52.32.43		Base		AT-8100L/8POE	E	A04385G133400029	2.2.5.0	
10.52.32.23		Base		x610-48Ts-POE+	X1-0	A04431H101200012	5.4.3-3.11	
10.52.32.23		Expansion	Bay1	AT-StackXG	A-0	N/A		
10.52.32.23		PSU	PSU1	PWR800	X1-0	PWR0854		
10.52.32.42		Base		IX5-28GPX	A-0	A25DD8027	5.4.4-0.4	eccd.6daa.c8a2
10.52.32.42		PSU	PSU1	PWR800	D-0	A21LD900V		
10.52.32.24		Base		AT-8100S/24POE	A	A04480G113100076	2.2.2.3	
10.52.30.2		Base		AT-AR745	M3-0	58793416	2.9.2-13 26-Sep-2013	
10.52.30.2		PIC	0	AT-AR026-00 PIC 10/100 Eth	M2-0	58471126		
10.52.30.2		PIC	1	AT-AR021(S)-00 PIC BRI(S)	M1-0	58817455		
10.52.30.15		Base		AT-AR770S	M3-0	G1F77502H	2.9.2-09 21-Aug-2012	
10.52.30.15		PIC	0	AT-AR020-00 PIC E1/T1 PRI	M3-0	58467617		

FIGURE 7-28 Example AlliedWare Plus Inventory Report

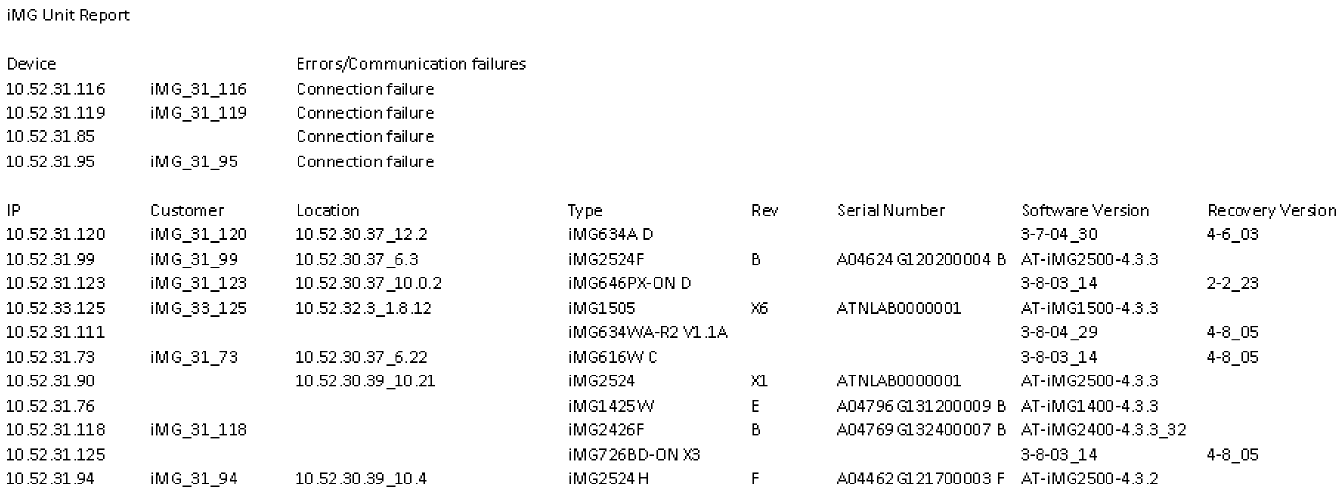


iMAP Card Report

Device	Description	Shelf Serial Number	Shelf CLEI Code	Shelf MAC	Hostname	Location
10.52.30.35	Allied Telesis 10400 Multiservice Access	ATNLAB4030200126	<unknown>	00:0C:25:00:01:D8	iMAP35	NMS_B7
10.52.30.34	Allied Telesis 9400 Multiservice Access	0056194030800030 A1	VAMD200HRA	00:0C:25:00:F8:74	Dot34	NMS_B7
10.52.30.37	Allied Telesis 9810 Multiservice Access	A041014094000012 B	NOCLEICODE	00:0C:25:1F:80:3C	dot37	NMS_B7
10.52.30.36	Allied Telesis 10700 Multiservice Access	ATNLAB4030200512	VAMD200HRA	00:0C:25:00:06:76	dot36	NMS_B7
10.52.30.39	Allied Telesis Switchblade x3112 - 12 Slot	A042764102400032	<unknown>	EC:CD:6D:03:11:4B	DOT39	NMS_C4
10.52.30.38	Allied Telesis 9100 Multiservice Access	A02928S060100039 A	NOCLEICODE	00:0C:25:0B:49:F4	dot38	NMS_B7
10.52.30.33	SW release predates Inventory Mgmt support					

Device	Slot	Type	State	Model Number (Revision)	Serial Number	CLEI Code	
10.52.30.35	0	GE3	UP-UP-Online	TN-301-A (Rev A4)	0056224040400035 A1		
10.52.30.35	1	GE3	UP-UP-Online	TN-301-C (Rev A)	A043994130800003 A	NOCLEICODE	
10.52.30.35	2/4	CFC56	UP-UP-Online (Active)	TN-407-A (Rev H0)	ATNLAB4040302467		
10.52.30.35	3	FC7	UP-UP-Online	TN-E004-A (Rev A3)	0056404031000022 A3		0
10.52.30.35	5	FX20	UP-UP-Online	TN-139-A (Rev X9)	A03897M072400005 X4	NOCLEICODE	
10.52.30.35	6	GE8	UP-UP-Online	TN-117-B (Rev E)	A039784084000004 D	NOCLEICODE	
10.52.30.35	7	CES8	UP-UP-Online	TN-119-B (Rev D)	A039814085000035 D	NOCLEICODE	
10.52.30.35	8	ADSL24B	UP-DN-Reset	- (Rev -)	uninitialized		
10.52.30.35	9	NTE8	UP-UP-Online	TN-125-A (Rev K)	A028604093600002 K	NOCLEICODE	
10.52.30.35	11	FE10	UP-UP-Online	TN-102-A (Rev X9)	ATNLAB4030200414	VAUCAAWGTA	

FIGURE 7-29 Example iMAP Inventory Report



iMG Unit Report

Device		Errors/Communication failures
10.52.31.116	iMG_31_116	Connection failure
10.52.31.119	iMG_31_119	Connection failure
10.52.31.85		Connection failure
10.52.31.95	iMG_31_95	Connection failure

IP	Customer	Location	Type	Rev	Serial Number	Software Version	Recovery Version
10.52.31.120	iMG_31_120	10.52.30.37_12.2	iMG634A D			3-7-04_30	4-6_03
10.52.31.99	iMG_31_99	10.52.30.37_6.3	iMG2524F	B	A04624G120200004 B	AT-iMG2500-4.3.3	
10.52.31.123	iMG_31_123	10.52.30.37_10.0.2	iMG646PX-ON D			3-8-03_14	2-2_23
10.52.33.125	iMG_33_125	10.52.32.3_1.8.12	iMG1505	X6	ATNLAB0000001	AT-iMG1500-4.3.3	
10.52.31.111			iMG634WA-R2 V1.1A			3-8-04_29	4-8_05
10.52.31.73	iMG_31_73	10.52.30.37_6.22	iMG616W C			3-8-03_14	4-8_05
10.52.31.90		10.52.30.39_10.21	iMG2524	X1	ATNLAB0000001	AT-iMG2500-4.3.3	
10.52.31.76			iMG1425W	E	A04796G131200009 B	AT-iMG1400-4.3.3	
10.52.31.118	iMG_31_118		iMG2426F	B	A04769G132400007 B	AT-iMG2400-4.3.3_32	
10.52.31.125			iMG726BD-ON X3			3-8-03_14	4-8_05
10.52.31.94	iMG_31_94	10.52.30.39_10.4	iMG2524H	F	A04462G121700003 F	AT-iMG2500-4.3.2	

FIGURE 7-30 Example iMG Unit Report

7.6.2 Example: Obtaining iMAP 9810 CFC100 MAC Addresses

This example demonstrates how to produce a report that lists the MAC addresses for all of the CFC100 cards in a network. You can use this output to obtain Allied Telesis release activation license keys for the cards.

To obtain a list of CFC100 card MAC addresses:

1. From the **Tools** menu, go to **Inventory Report Utility**. The **Inventory Management** box appears.
2. For **Report Name**, select **iMAP Card Report**.

3. In the **Select Criteria** field, enter the match criteria for the iMAP 9810 CFCs in your network. For example, if they are all in the same subnet, enter the subnet. If they follow a similar name pattern, enter the common part of the name.
4. In the **Simultaneous #Devices** field, enter the maximum number of devices to query concurrently.
5. Click **OK**.
6. When the report opens, delete all columns except **Base MAC Address**.
7. Delete any rows in the report that are not iMAP 9810 CFCs.
8. Save the report as a .csv file as required by Allied Telesis for license key generation.

7.7 AlliedView NMS License Manager

The following applies to the NMS license manager:

- The license key is associated with the customer who has registered the license rather than the hardware where the key was installed.
- Licensing can include the following:
  - whether the license running NMS is temporary (time limit)
  - the maximum number of nodes allowed
  - allowing access to RADIUS and max number of clients allowed
  - allowing access to the Northbound Interface.
- The details of the license key are encrypted and kept in xml format as AT_License.conf in the Conf subdirectory.

The process of obtaining a license is similar to previous releases and includes the following:

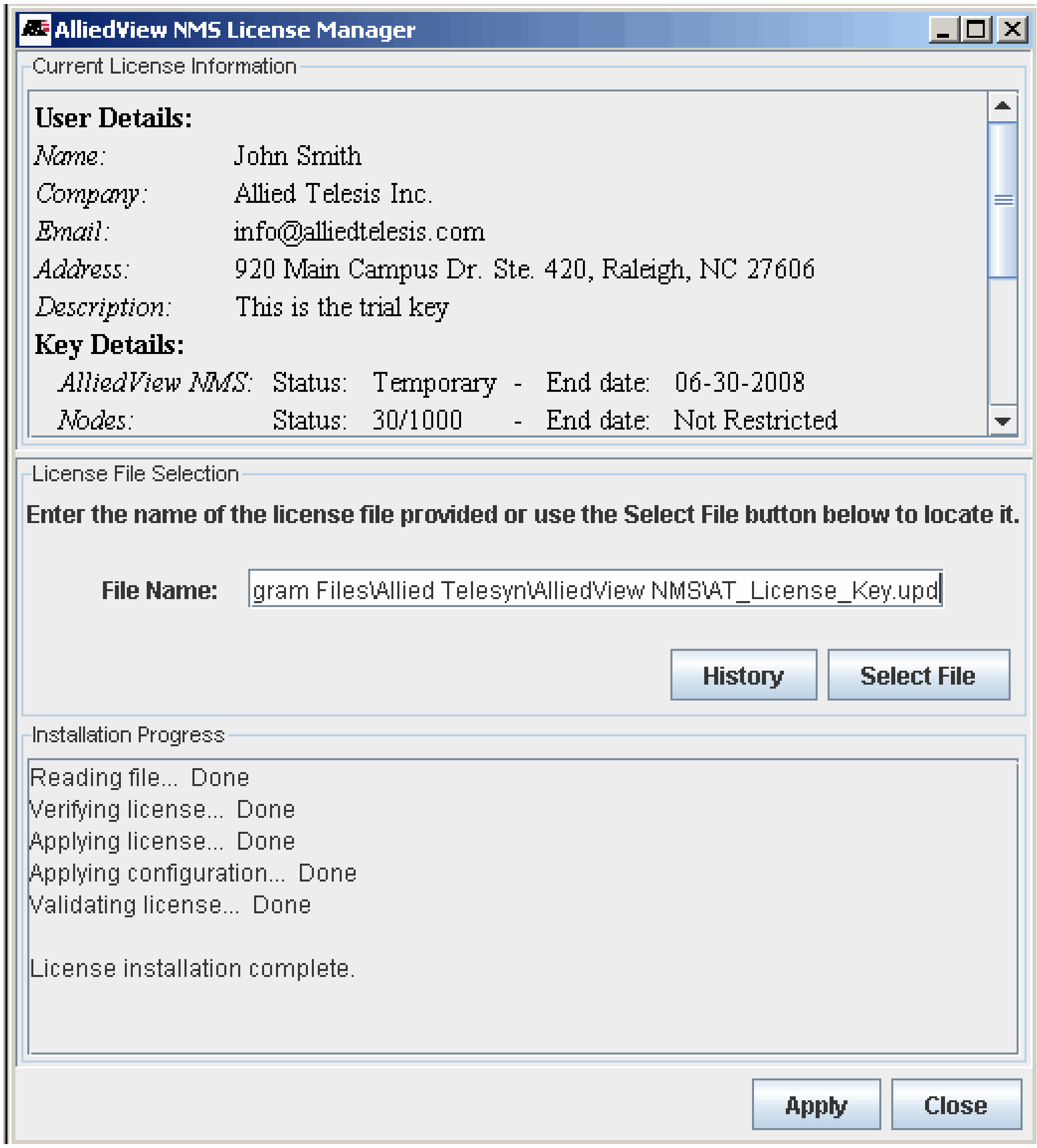
1. The customer fills out a form in which all relevant information is filled in and is sent to Allied Telesis.
2. Allied Telesis receives the form and encodes the customer information and license privileges in the file AT_LicenseKey.upd.
3. The customer receives the file and places it on the NMS server.
4. The customer uses the License Manager GUI to select this file and apply the license.
5. The customer can look at the Status Monitoring Tool and look at the License Keys node to review the Licensed User Information panel.

7.7.1 Installing a License (Using the License Key Manager)

The License Key Manager can be used to apply the license key. The new key can be installed while the server is running without affecting other services. Some sections of the key will take effect immediately (e.g. node limit), and others will take effect after the next server restart.

When a new key is installed with its separate components, it will update previous key of the same component. However, existing product or component keys that are not included in the new key will not be updated. Also, the installed key will not be removable (i.e. there will be no tools to uninstall a key) but a new key can be created to reset the unwanted key to original or any other values.

Refer to the following figure, which show the License Manager Tool.



User Details:

Name: John Smith
Company: Allied Telesis Inc.
Email: info@alliedtelesis.com
Address: 920 Main Campus Dr. Ste. 420, Raleigh, NC 27606
Description: This is the trial key

Key Details:

AlliedView NMS: Status: Temporary - End date: 06-30-2008
Nodes: Status: 30/1000 - End date: Not Restricted

Enter the name of the license file provided or use the Select File button below to locate it.

File Name: gram Files\Allied Telesyn\AlliedView NMS\AT_License_Key.upd

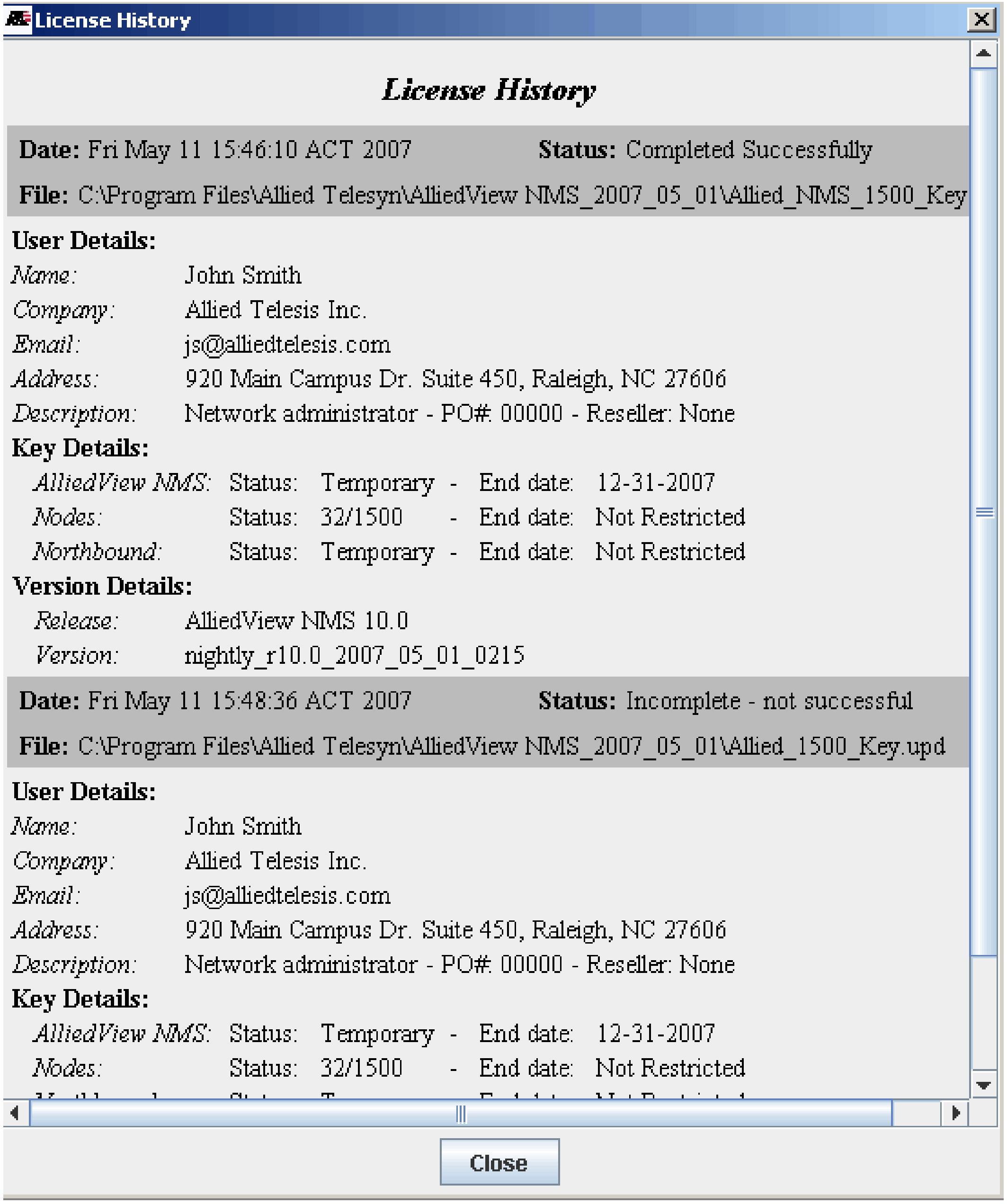
```
Reading file... Done
Verifying license... Done
Applying license... Done
Applying configuration... Done
Validating license... Done

License installation complete.
```

FIGURE 7-31 License Manager Tool

The license key installation user interface has three main sections:

- Current License Information (Top): This section has information on the key that is already installed. It displays the license status including user information, product and all components being licensed.
- License File Selection (Middle): This section allows the user to select the license file to be applied. The license key file is expected to be on the server and contain the correct extension and the file chooser can be used to select a file from the file system mounted in the server.
- Installation Progress (Bottom): This section will display status of the current license installation and the information printed here will be very useful if the installation fails.

There is also a License Key History (Separate panel): This is launched by selecting the **History** button to display the history of all licenses that have been installed on the system in the past. Refer to the following figure.



License History

Date: Fri May 11 15:46:10 ACT 2007 **Status:** Completed Successfully

File: C:\Program Files\Allied Telesyn\AlliedView NMS_2007_05_01\Allied_NMS_1500_Key

User Details:

Name:	John Smith
Company:	Allied Telesis Inc.
Email:	js@alliedtelesis.com
Address:	920 Main Campus Dr. Suite 450, Raleigh, NC 27606
Description:	Network administrator - PO#: 00000 - Reseller: None

Key Details:

AlliedView NMS:	Status:	Temporary	-	End date:	12-31-2007
Nodes:	Status:	32/1500	-	End date:	Not Restricted
Northbound:	Status:	Temporary	-	End date:	Not Restricted

Version Details:

Release:	AlliedView NMS 10.0
Version:	nightly_r10.0_2007_05_01_0215

Date: Fri May 11 15:48:36 ACT 2007 **Status:** Incomplete - not successful

File: C:\Program Files\Allied Telesyn\AlliedView NMS_2007_05_01\Allied_1500_Key.upd

User Details:

Name:	John Smith
Company:	Allied Telesis Inc.
Email:	js@alliedtelesis.com
Address:	920 Main Campus Dr. Suite 450, Raleigh, NC 27606
Description:	Network administrator - PO#: 00000 - Reseller: None

Key Details:

AlliedView NMS:	Status:	Temporary	-	End date:	12-31-2007
Nodes:	Status:	32/1500	-	End date:	Not Restricted

FIGURE 7-32 License History

When the user selects the Apply button, the selected file is read and checked, installed, and then verified. If there is an error during these steps, the installation will stop. If there are no errors, the key is also stored at another location if needed later for recovery.

7.7.2 Installing a License (Using the Console Mode)

License keys can also be installed and viewed in console mode where all menu options and selections are displayed and entered on a command line and GUIs will not be launched. This mode can be useful when graphical display to the NMS server is not available.

The same script will be used for launching a console mode installation using selected options with the `AT_LicenseInstaller.bat` command.

```
cd <NMA_HOME>/bin
AT_LicenseInstaller.bat -help
Printing help: -help

 Usage (all parameters are optional):
   AT_LicenseInstaller [options]
   Where options are:
    -help  - Print this message (cannot be used with other
   options)
    -g     - Run in GUI mode (default and all other options
   are ignored)
    -c     - Run in console mode (other options may be added)
   Parameters below can only be used in console mode (-c) if
   needed to bypass text menu options.
    -s      - Display current license key status
    -h      - Display license key installation history
    -i ...  - Install a new license key (license file must be
              specified)
```

Note that all options can be passed on a command line when running the installer or the installer can be executed with the `- c` option and others can be selected from the key installation menu. This flexibility allows calling the license key installer from other programs in special circumstances if needed to bypass instructions menus.

```
============================================================
              AlliedView NMS License Manager
============================================================
AT_LicenseInstaller.bat -c
Please select from the license key menu below using the characters on the left to continue...

   S - Display current key Status
   H - Display key installation History
   I - Install new license key
   Q - Quit (Exit)
Select an option:
```

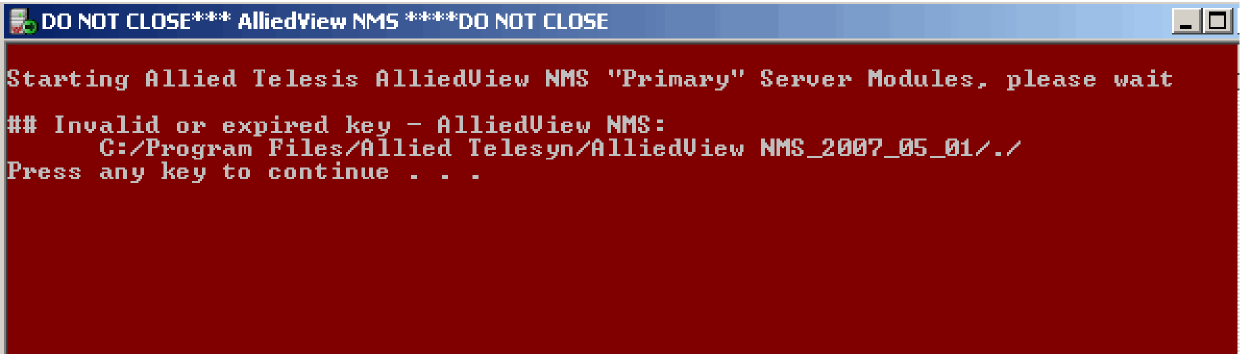
Options from the menu above will display the same information as when the GUI is used and the selections will also perform the same function as when GUI is used.

7.7.3 Verifying the License After Installation

7.7.3.1 Product Validation

Validating the product key has the following scenarios:

- **Server startup** - If the product key is found to be invalid the server will stop, and the following appears. This occurs because the key is invalid or has expired.



```
Starting Allied Telesis AlliedView NMS "Primary" Server Modules, please wait

## Invalid or expired key - AlliedView NMS:
      C:/Program Files/Allied Telesyn/AlliedView NMS_2007_05_01/./
Press any key to continue . . .
```

FIGURE 7-33 License Expired/Invalid at Server Startup

- **Server runtime**: Once the server has started, and if the key is found to be invalid, the server is stopped. There will be warning messages in the logs that allow the user to correct the problem before the server is stopped.

7.7.3.2 Viewing Licensed User Information

Once the license is applied, select *Tools -> Status Monitoring*, then select **License Keys** to see the license information for the customer. The following subsections go through the license features.

7.7.3.3 Node Limit Validation

There is already a Node limiting feature, and this is being included with the License Manager in Release 10.0. If the new license includes this feature and a new maximum count, it will not be a replacement to current maximum value, and when the key is applied the old value will be replaced with new value. Therefore, Allied Telesis and the customer should compare records to ensure there is agreement on the value to be used.

The maximum node count can also be decreased with the License Manager, setting the value lower than what was set in 9.0. If there are already more nodes than the new value, the extra nodes will not be deleted but new nodes will not be allowed until some are deleted to make the count lower than new value.

This feature includes the option to have expiration dates so that more nodes can be added for specific time, and the value will automatically reset to default value when the time expires. Also in normal run the maximum node limit can be reset to a default value when the key is detected to be invalid or expired.

7.7.3.4 Northbound Interface Validation

Access to Northbound interface APIs can be time-based, and access to the APIs is blocked when the time expires. Note that when this occurs, all APIs are blocked. (For Northbound Interface, refer to Section "Northbound Interface" on page 1117)

7.7.3.5 Maximum Allowable Client Logins

Prior to Release 10.0, the maximum available active clients was limited to five (5) on a single NMS server. (This was the default.) In release 10.0, this maximum can be increased to 15.

7.7.3.6 RADIUS License Information

The RADIUS feature allows access to RADIUS server authentication, and the attributes are listed.

7.7.4 Viewing the License Configuration

When the NMS first starts up, the initial splash screen will include text on licensing. This information is also included in the About menu item.

The License Key information is also included in the Status Monitoring Panel. Refer to "Status Monitoring" on page 143.

7.7.5 Migrating Existing Licenses

NMS License Keys issued prior to R10.0 will no longer be valid. Therefore effective with NMS R10.0, all customers upgrading from R9.0 to R10.0 will be required to get a new license key from Allied Telesis.

Upgrading a properly licensed NMS R9.0 server to R10.0 will result in the license status being placed back into Evaluation status. Allied Telesis is making every effort to contact all existing customers with new R10.0 compatible license keys to minimize customer inconvenience.

7.8 File Keys to Identify Downloadable Files

As explained in Section "Standard Load Software Configuration" on page 298, Software Configuration is an MDTI application that downloads OS releases onto supported devices/components. Since there are many steps and constraints involved in this operation, the MDTI application is a considerable simplification of the process, especially when downloading to multiple devices. The application uses a file on the NMS to identify the files that can be downloaded on devices according to their device types. This file also encodes file relationship constraints.

In previous releases, the data store was static within an NMS release, which meant new OS releases delivered after a particular NMS release could not be downloaded to existing devices. The Custom Software Download feature gives users a safe way to modify the data so newer OS releases can be downloaded to existing devices without waiting for a new NMS release or patch.

Note: NMS applications are not necessarily expected to support devices running advanced releases but will make a best effort in order to do so.

Using the Custom Software Download feature, explained in Section "Custom Load Software Configuration" on page 303, the user can modify the file that stores the **OS release files**. These custom (usually newer) **release** files must be already loaded in the following path; NMS-HOME/swdownload

The file properties consist of required file keys and their names. The names are OS release files and their required resources, if any. The required file keys vary according to the specific device type.

In using the Custom Software Download feature, the user selects an existing device type (new device types are not supported). The user then selects file names from the files in the above paths for each type-specific file key. See Table 7-5 for example supported device types and their required file keys.

If the Load already contains an entry for the selected device type, its file properties will be replaced by the new selections, otherwise the new entry will be added to the selected Load.

Caution: Devices will fail if the wrong file is used for the wrong purpose when downloading a new release. Standard loads have been tested for correct configurations. Moreover, software upgrades may require updating of loads in a specific sequence to ensure data configuration integrity. Custom loads are usually created and used by Network Administrators, and they must use this feature with extra caution

TABLE 7-5 Example Device Type File Keys

Component Type	Component Category	Required File Keys
Telesis (TN) - ADSL24AE - ADSL48 - FX20 - CFC24[a] - CFC56 etc.	iMAP	 NEW_ADSL24AE_LOAD NEW_ADSL48A_LOAD NEW_FX20_LOAD NEW_CFC24_LOAD NEW_CFC56_LOAD etc.
Rapier Types	Rapier	NEW_RELEASE NEW_PATCH NEW_GUI_RESOURCE NEW_HELP

[a] The CFC loads are for the cfc24univ load type. Refer to the Allied Telesis Component Specification for more details.

7.9 Log Files for Debugging the AlliedView NMS Server

This list contains log files that have useful information in debugging NMS problems; The list can be used by support to collect debugging logs if there is a problem in the NMS server.

- NMS logs (Server logs):
  - <AlliedViewNMS>/logs/* (all files in this directory)
- InstallShield Logs (Installer/Uninstaller/Key logs):
  - <AlliedViewNMS>/log.txt
- Webserver logs (Apache/Tomcat logs):
  - <AlliedViewNMS>/apache/logs/* (all files in this directory)
  - <AlliedViewNMS>/apache/tomcat/logs/* (all files in this directory)
- Database logs (MySQL):
  - <AlliedViewNMS>/mysql/data/mysql.err
- Upgrade logs (Service Packs logs):
  - <AlliedViewNMS>/Patch/logs/* (all files in this directory)
  - <AlliedViewNMS>/Patch/*.txt (all text files in this directory)
  - <AlliedViewNMS>/Patch/*.xml (all XML files in this directory)
- Client logs if available
  - <NMS client console has a save to file option>
  - <Other client logs e.g. dialog error messages>
- Others:
  - <AlliedViewNMS>/AT_revision.txt (Build release information)

7.10 Status Monitoring

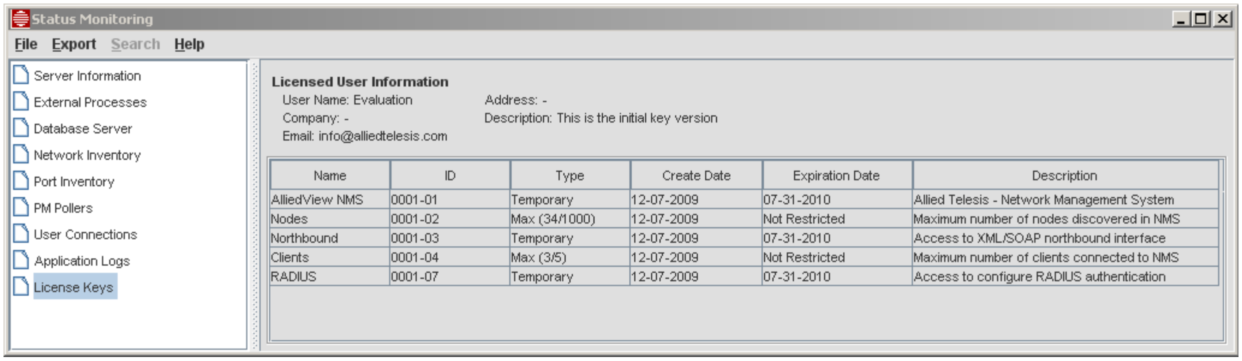
The Status Monitoring feature allows you to track the connections, processes, and overall status of the server(s) that make the AlliedView NMS,

To access this feature, select *Tools -> Status Monitoring* from the Main Menu. The main window appears, as shown in the following figure.

Using the Export Option, the user can select either Export Summary Information (all of the panels) or Export Panel Information (the current panel) and export these as:

- An html file to the browser
- A bracket-delimited, comma-separated file to the selected server.

Note: Initially, the rows are sorted by the table category but the user can change the order by clicking on the appropriate column heading.



Licensed User Information

User Name: Evaluation

Company: -

Email: info@alliedtelesis.com

Address: -

Description: This is the initial key version

Name	ID	Type	Create Date	Expiration Date	Description
AlliedView NMS	0001-01	Temporary	12-07-2009	07-31-2010	Allied Telesis - Network Management System
Nodes	0001-02	Max (34/1000)	12-07-2009	Not Restricted	Maximum number of nodes discovered in NMS
Northbound	0001-03	Temporary	12-07-2009	07-31-2010	Access to XML/SOAP northbound interface
Clients	0001-04	Max (3/5)	12-07-2009	Not Restricted	Maximum number of clients connected to NMS
RADIUS	0001-07	Temporary	12-07-2009	07-31-2010	Access to configure RADIUS authentication

FIGURE 7-34 Status Monitoring Panel

7.10.1 Status Table

TABLE 7-6 Status Monitoring Window

Status Type	Field	Description
Server Information	Host Name	Host name of the server
	IP Address	IP address of the server
	Type	Server type (PRIMARY)
	Port	Port used for connection to the server
	State	Last observed state of the server (Up if connection working, Down server fails
	Uptime	Time since the server was last started
	CPU Time	Total processor time used by the server since it was started
	Memory Usage (K)	Current working memory, in kilobytes
	Forwarding	TBS
External Processes	Name	Process Name
	Program Name	The executable filename
	PID	Process ID
	Usage (%)	Amount of CPU usage currently allocated to the process
	State	The last observed state of the process. The state can be: - Up – if the process is working - Down – if the process is not working
DataBase Server	Connection Information	Provides basic information about the connection to the database. - Host Name - the hostname of the machine where the database server runs. - Port - the port used for the connection to the database server. - User Name - the user name used for the current connection to the database server.
	Database Information	Provides basic information about the database used by the application. - Product - the name and version of the database server used by the application. - Driver - the name and version of the database driver used to connect to the database server. - URL - information about the URL used by the database server.
	Table Columns	Each row contains: - Name - the name of the table. - Rows - the number of rows. - Data Length (B) - the length of the data file, in bytes. - Index Length (B) - the length of the index file, in bytes. - Update Time - when the data file was last updated.
	# of Available Tables	The total number of available tables in the database

TABLE 7-6 Status Monitoring Window (Continued)

Status Type	Field	Description
Network Inventory	Table Columns	Each row contains: - Type - type of network objects. Note: New network objects will be automatically added to the list. - Discovered - the total number of discovered objects. - Managed - the total number of managed objects. - Unmanaged - the total number of unmanaged objects.
Port Inventory	Tables for iMAPs. Ports, and iMG/RGs	Allows the administrator to see in one screen the total numbers of each type of iMAP, iMG/RG, and Port. For each port type, there is also the number of those ports that have been provisioned with a Customer ID (and should therefore be provisioned and passing customer traffic). The counts can also be derived from the Network Inventory tables, but using this tool provides all of the counts in one screen.
PM Pollers	Summary	This provides basic information about the PM Pollers. - Total Active Polled Data - the total number of polling objects that are currently collecting statistics. - Total Number of Devices Polled - the total number of devices that have active polling objects. - Polling Interval (Shortest/Longest) - the time interval for periodic data collection.

TABLE 7-6 Status Monitoring Window (Continued)

Status Type	Field	Description
	Column Names	- Host Name - the host name of the device that have active polling object. - Type - the type of the device. - IP Address - the IP address of the device. - Polled Data - the name of the active polling object. - Polling Interval - he time interval for periodic data collection. - Polling Type - the type of the active polling object. The type can be: - Node – if the data identifier is scalar type: - Interface – if the data identifier has many instances - Multiple – if the data identifier has multiple instances - None – if other protocol is used other than SNMP - Save Collected Data - Indicates whether the data will or will not be stored. This can be: - Yes – if the data will be saved - No – if the data will not be saved - Log Directly This indicates if the data will or will not be stored in a text file. This can be: - Yes – if the data will be saved to a text file - No – if the data will not be saved to a text file

TABLE 7-6 Status Monitoring Window (Continued)

Status Type	Field	Description
User Connections	Active User Connection	Displays all active user connections to the server. Each row contains: - User Name - the name of the currently connected user. - Total - the number of connections a user has currently established to the server. Selecting a user name will display the individual threads of that user in the lower box.
	User Thread	Each row contains: - User Name - the name of the currently connected user. - Host Name - the host name or IP address of the client in which the user used to connect to the server. - Type - the type of client used by the user to connect to the server. - Time - the time since the user was connected to the server.
	Telnet Sessions	This provides basic information about the CLI resources. - Total Active Connections - the total number of connections that have been established. - Maximum Number of Connections - the total maximum number of connections that can be established. - Pooling Sharing - the pooling flag common to telnet sessions. This can be: - Enabled – if the pooling sharing is enabled - Disabled – if the pooling sharing is disabled
Application Logs	Trace Log	This displays the trace logs. - Trace (Text Area) - displays the trace messages from '<installed location>/logs/ trace.txt.0' file. This is a read-only field.
	Standard Log	This displays latest standard output/error log file. - Output (Text Area) - displays the standard output messages from '<installed location>/logs/nmsout.txt' file. This is a read-only field. - Error (Text Area) - displays the standard error messages from '<installed location>/logs/nmserr.txt' file. This is a read-only field.
	Server Log	This displays latest standard output/error log file. - Output (Text Area) - displays the standard output messages from '<installed location>/logs/nmsout.txt' file. This is a read-only field. - Error (Text Area) - displays the standard error messages from '<installed location>/logs/nmserr.txt' file. This is a read-only field.
	System Log	This displays the syslog.txt file

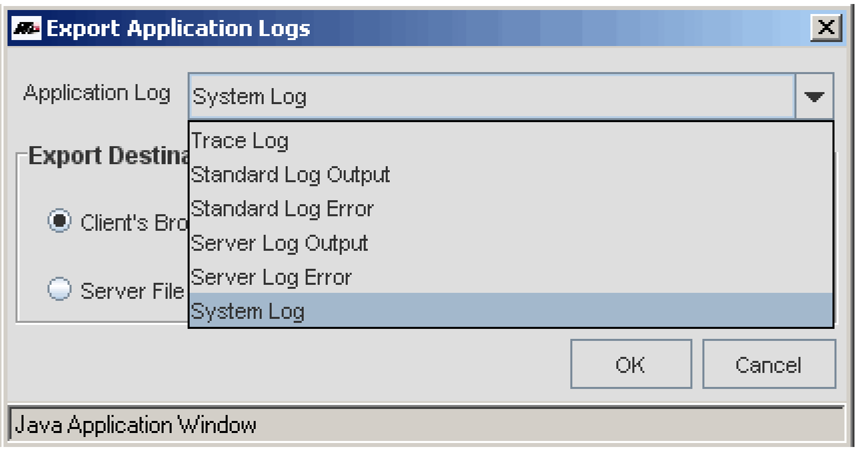
TABLE 7-6 Status Monitoring Window (Continued)

Status Type	Field	Description
License Keys	Name	Name of the License Feature. Up to four features can be listed.
	ID	
	Type	Depending on the feature, this can mean whether the feature is temporary or has a certain limit
	Create Date	When the feature was installed
	Expiration Date	When the feature expires or Not Restricted (permanent)

7.10.2 Menu Options (Export)

The Export menu item has the following options:

- **Export Summary Information** - This is a summary report of all the areas of Status Monitoring.
- Export panel Information - This is what appears in the panel that is currently being viewed. The one exception to this is for Application logs, where there is a pull-down to select the type of log, as shown in the following figure.



Export Application Logs

Application Log: System Log

FIGURE 7-35 Selecting Type of Logs for Export

- Archive Logs - This is an archive file that contains all log types and can be filtered by date.

The administrator then has the option to view the data in a local browser or to export the data by selecting the Browse button to provide a filename and file type what will be placed in the Status directory.

7.11 Downloading Device Files

7.11.1 Standard versus Custom Loads

Device loads that are transferred to the NMS and then loaded onto devices are in two main types:

- Standard load - This is usually a set of device loads that is pre-packaged for a release and is known to be compatible with certain NMS loads. Starting in NMS release 10.0, these are not included with the NMS software, but are available on either a CD provided by Allied Telesis or are on an FTP server that is available to Allied Telesis customers.
- Custom load - These are specific loads for a device or device type. Although NMS compatibility is not guaranteed, these are usually incremental updates and so should be compatible. These loads are available on Allied Telesis websites.

Before either type can be loaded onto devices, they must exist in the `<NMS-Home>swdownload` directory. Moreover, **the firmware and associated xml files must both be included**. The process to achieve this for standard and custom loads is as follows:

- Standard Loads
  - The Load Import tool (explained in "Load Import GUI (Standard Loads)" on page 149), allows the user to place both the firmware and xml files into the swdownload directory in a easy to use GUI format.
  - The user can manually download the files and unzip them before placing them into the swdownload directory. This method would be used when the NMS is on a Linux platform.

Note: For the manual download, ensure that the files are unzipped only once.

- Custom Loads - The user must download the files manually, and then use the Create Custom Load option that is part of the Software Configuration application (refer to "Custom Load Software Configuration" on page 303).

Refer to the following figure that shows the steps that are followed.

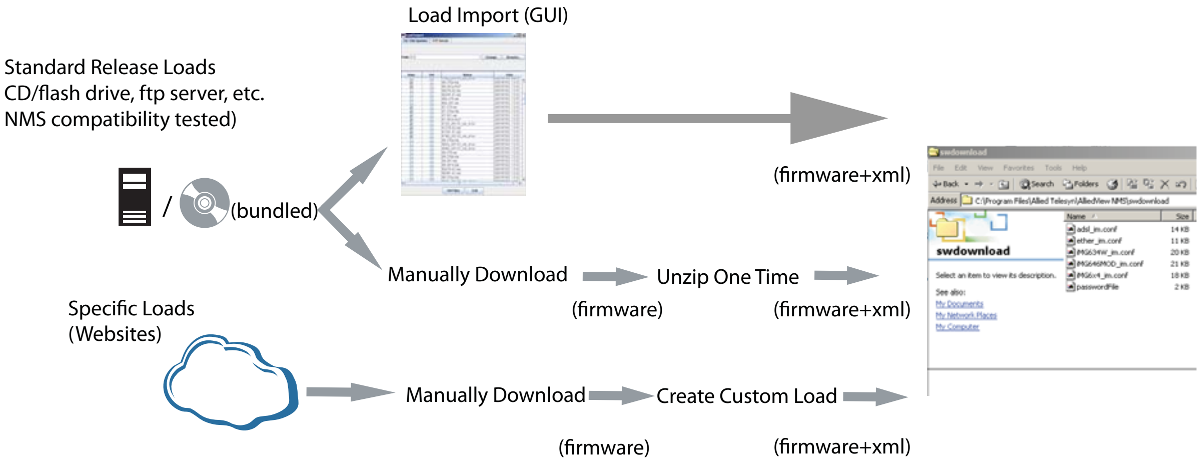


FIGURE 7-36 Download Overview

7.11.2 Load Import GUI (Standard Loads)

The NMS uses a tool to upload firmware bundles. The tool is located in the NMS server bin directory.

To run the tool on Windows:

- Double-click on `AT_FwLoadImport.bat`

To run the tool on Linux:

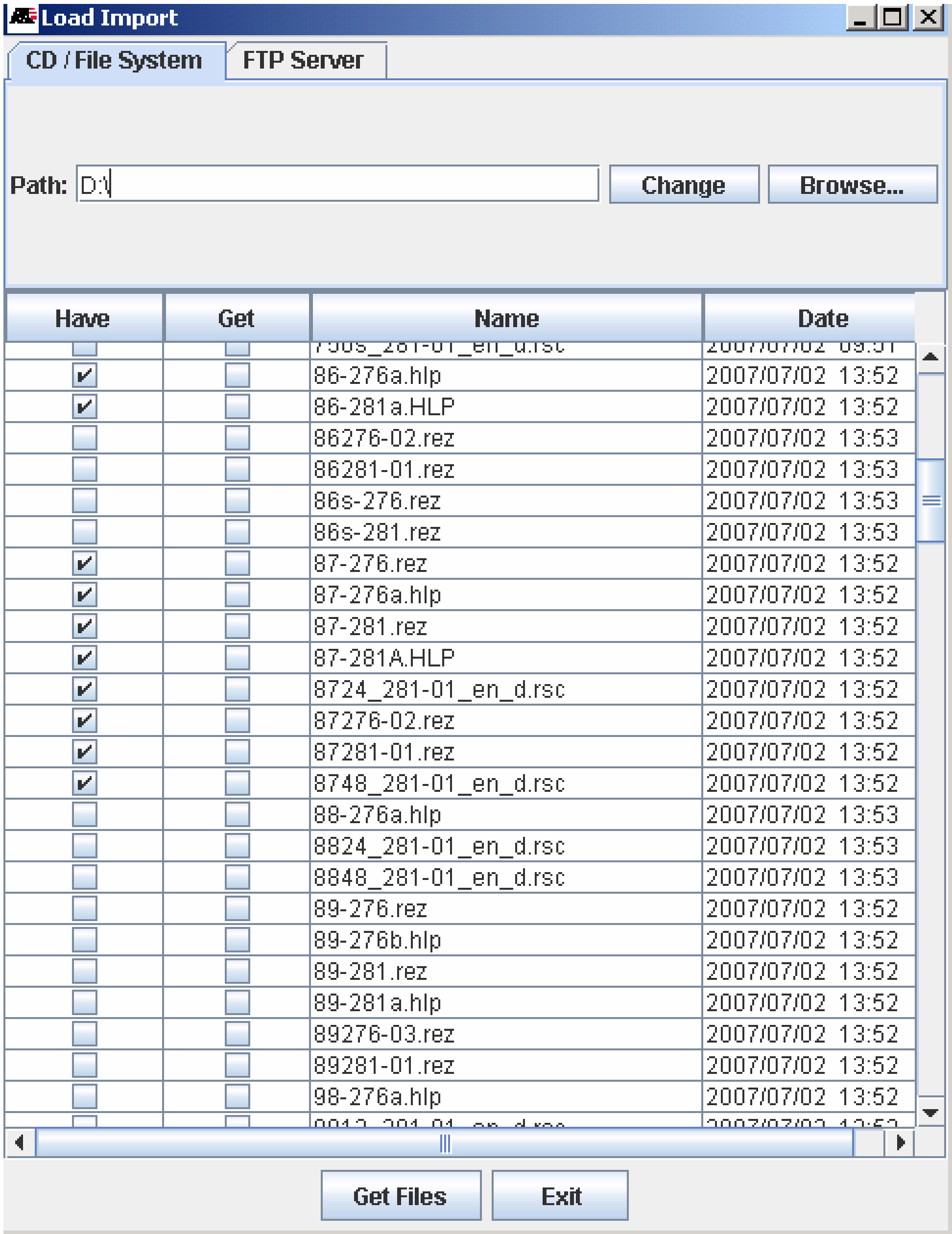
- Execute `AT_FwLoadImport.sh`

The tool can be used to load firmware into the NMS from either a CD (or file system) or an FTP server. The tool displays a list of files available for download, their timestamps, and whether or not they're already loaded into the NMS. By checking the “Get” boxes, files can be selected for download. The **Get Files** button will load the selected files into the NMS. Loading progress is displayed in a popup window and zip files are unzipped as they're loaded.

Use the tab at the top to select a CD / File System download or an FTP Server download.

The CD / File System tab contains a Path field where a directory path can be entered. Either enter carriage-return or click the **Change** button to get a list of files available in that directory. Use the **Browse** button to popup a directory browser to point-and-click directory changes. Doubling-clicking will change the directory, update the file list, and leave the browser displayed so further directory changes can be selected.

The FTP Server tab also contains Host, Username, and Password fields to designate the FTP server and login credentials. The **Connect** and **Disconnect** buttons allow logging in and logging out of the FTP server. An initial directory can be entered into the Path field before connecting. Then once logged in the tool will immediately change to that directory. Further directory changes can be made the same way as in the CD / File System tab. Since FTP is remote, there may be delays updating the file listings with each directory change.



Path: D:\

Have	Get	Name	Date
☑	☐	86-276a.hlp	2007/07/02 13:52
☑	☐	86-281a.HLP	2007/07/02 13:52
☐	☐	86276-02.rez	2007/07/02 13:53
☐	☐	86281-01.rez	2007/07/02 13:53
☐	☐	86s-276.rez	2007/07/02 13:53
☐	☐	86s-281.rez	2007/07/02 13:53
☑	☐	87-276.rez	2007/07/02 13:52
☑	☐	87-276a.hlp	2007/07/02 13:52
☑	☐	87-281.rez	2007/07/02 13:52
☑	☐	87-281A.HLP	2007/07/02 13:52
☑	☐	8724_281-01_en_d.rsc	2007/07/02 13:52
☑	☐	87276-02.rez	2007/07/02 13:52
☑	☐	87281-01.rez	2007/07/02 13:52
☑	☐	8748_281-01_en_d.rsc	2007/07/02 13:52
☐	☐	88-276a.hlp	2007/07/02 13:53
☐	☐	8824_281-01_en_d.rsc	2007/07/02 13:53
☐	☐	8848_281-01_en_d.rsc	2007/07/02 13:53
☐	☐	89-276.rez	2007/07/02 13:52
☐	☐	89-276b.hlp	2007/07/02 13:52
☐	☐	89-281.rez	2007/07/02 13:52
☐	☐	89-281a.hlp	2007/07/02 13:52
☐	☐	89276-03.rez	2007/07/02 13:52
☐	☐	89281-01.rez	2007/07/02 13:52
☐	☐	98-276a.hlp	2007/07/02 13:52

FIGURE 7-37 Load Import for CD/File System

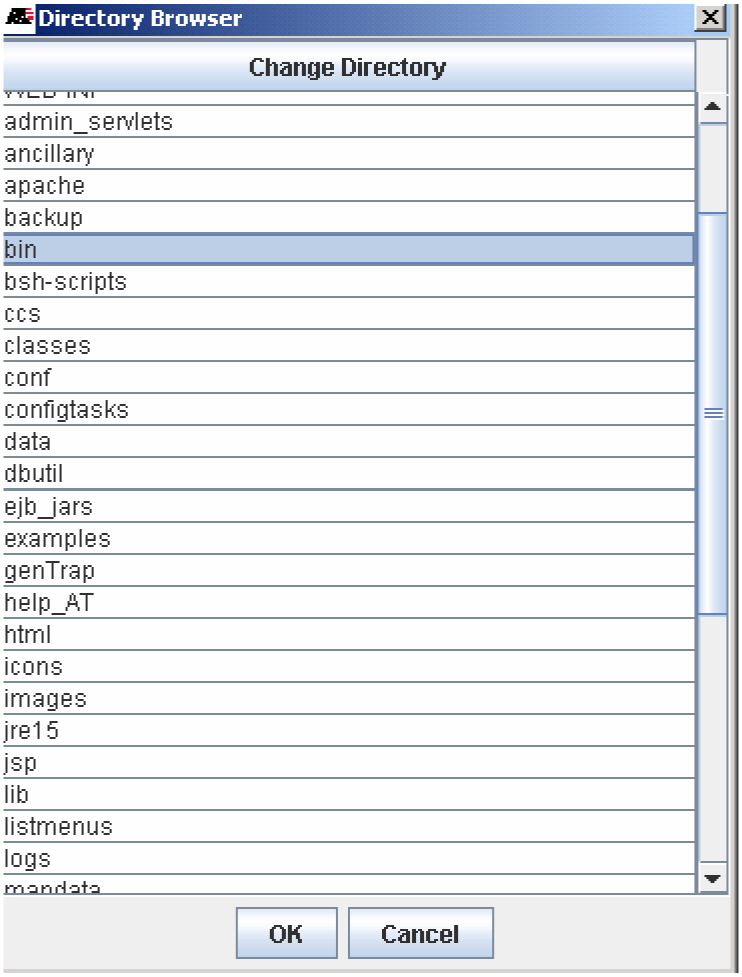
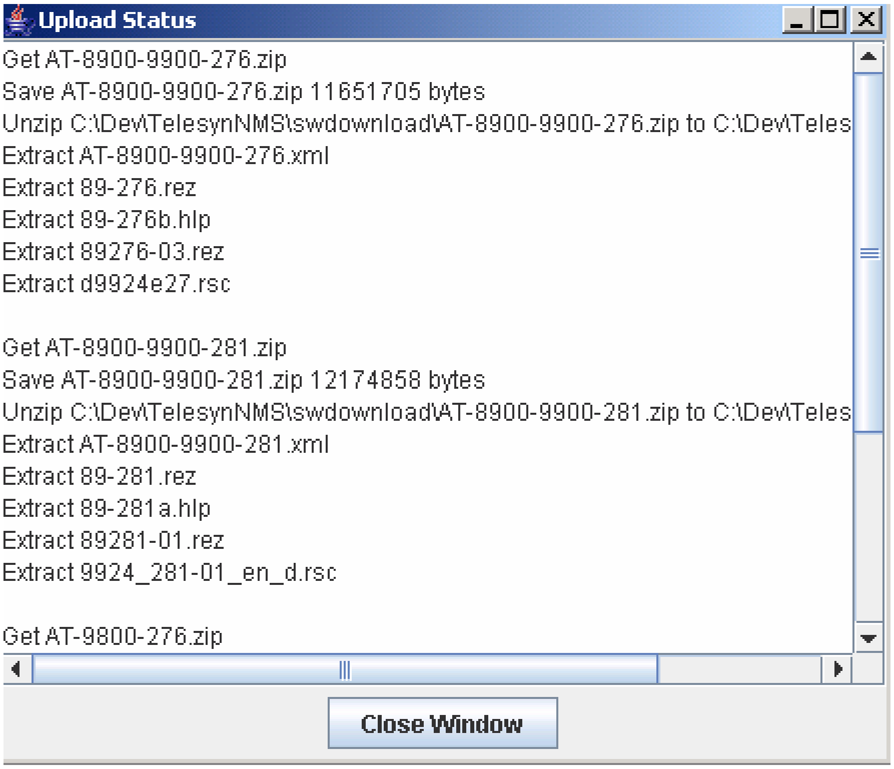
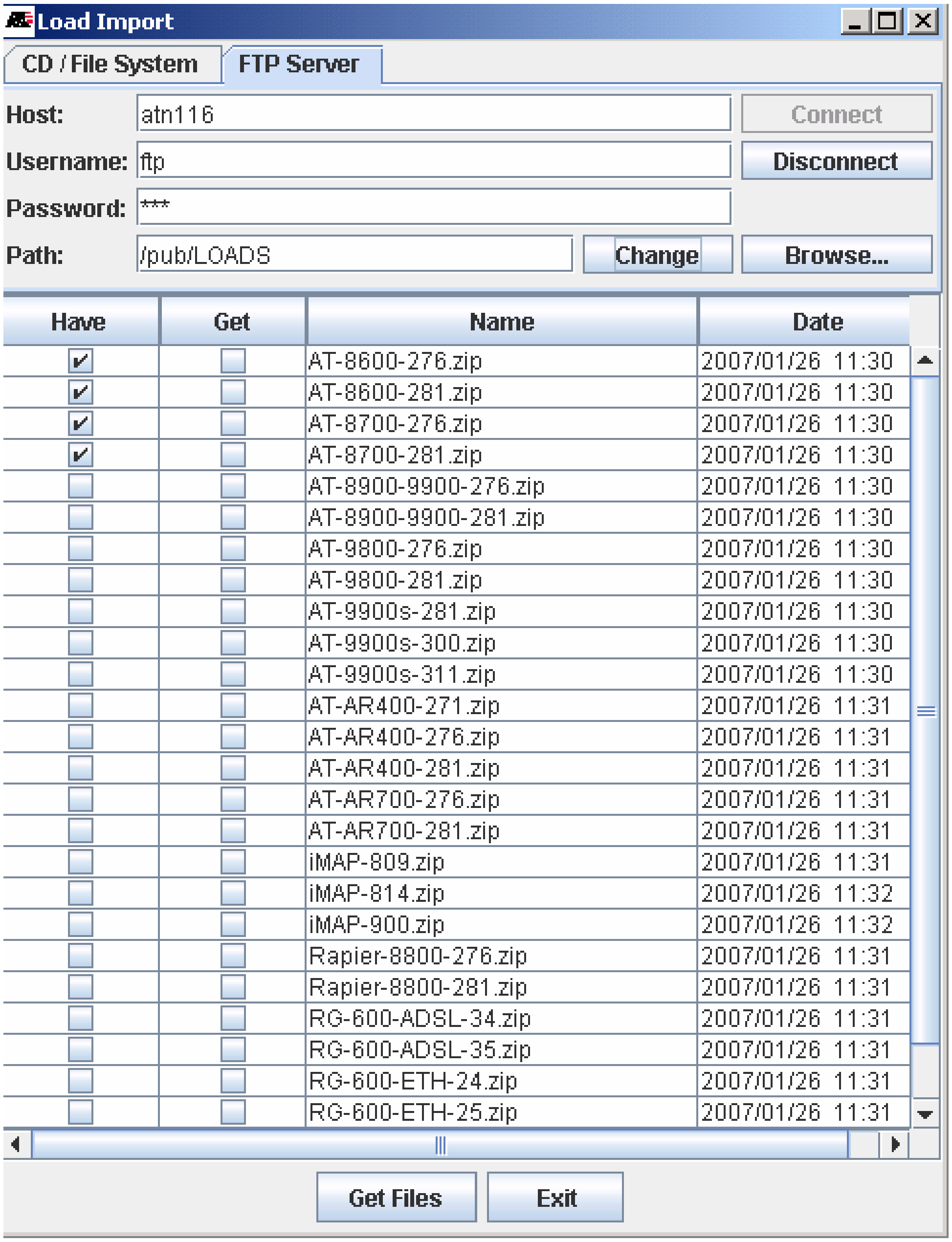


FIGURE 7-38 Changing Directories for Browsing



```
Get AT-8900-9900-276.zip
Save AT-8900-9900-276.zip 11651705 bytes
Unzip C:\Dev\TelesynNMS\swdownload\AT-8900-9900-276.zip to C:\Dev\Teles
Extract AT-8900-9900-276.xml
Extract 89-276.rez
Extract 89-276b.hlp
Extract 89276-03.rez
Extract d9924e27.rsc

Get AT-8900-9900-281.zip
Save AT-8900-9900-281.zip 12174858 bytes
Unzip C:\Dev\TelesynNMS\swdownload\AT-8900-9900-281.zip to C:\Dev\Teles
Extract AT-8900-9900-281.xml
Extract 89-281.rez
Extract 89-281a.hlp
Extract 89281-01.rez
Extract 9924_281-01_en_d.rsc

Get AT-9800-276.zip
```

FIGURE 7-39 Upload Status as Getting Files



Host: atn116

Username: ftp

Password: ***

Path: /pub/LOADS

Have	Get	Name	Date
☑	□	AT-8600-276.zip	2007/01/26 11:30
☑	□	AT-8600-281.zip	2007/01/26 11:30
☑	□	AT-8700-276.zip	2007/01/26 11:30
☑	□	AT-8700-281.zip	2007/01/26 11:30
□	□	AT-8900-9900-276.zip	2007/01/26 11:30
□	□	AT-8900-9900-281.zip	2007/01/26 11:30
□	□	AT-9800-276.zip	2007/01/26 11:30
□	□	AT-9800-281.zip	2007/01/26 11:30
□	□	AT-9900s-281.zip	2007/01/26 11:30
□	□	AT-9900s-300.zip	2007/01/26 11:30
□	□	AT-9900s-311.zip	2007/01/26 11:30
□	□	AT-AR400-271.zip	2007/01/26 11:31
□	□	AT-AR400-276.zip	2007/01/26 11:31
□	□	AT-AR400-281.zip	2007/01/26 11:31
□	□	AT-AR700-276.zip	2007/01/26 11:31
□	□	AT-AR700-281.zip	2007/01/26 11:31
□	□	iMAP-809.zip	2007/01/26 11:31
□	□	iMAP-814.zip	2007/01/26 11:32
□	□	iMAP-900.zip	2007/01/26 11:32
□	□	Rapier-8800-276.zip	2007/01/26 11:31
□	□	Rapier-8800-281.zip	2007/01/26 11:31
□	□	RG-600-ADSL-34.zip	2007/01/26 11:31
□	□	RG-600-ADSL-35.zip	2007/01/26 11:31
□	□	RG-600-ETH-24.zip	2007/01/26 11:31
□	□	RG-600-ETH-25.zip	2007/01/26 11:31

FIGURE 7-40 Load Import Tool for ftp Server

8. Security Administration

Security administration refers to permitting or restricting access to views and operations within the NMS. You can set permissions for individual users or assign users to groups and set permissions for each group. All users assigned to a group inherit the group permission settings.

8.1 Using Security Administration

To access the security administration utility, go to **Tools > Security Administration**. The Security Administration tool appears.

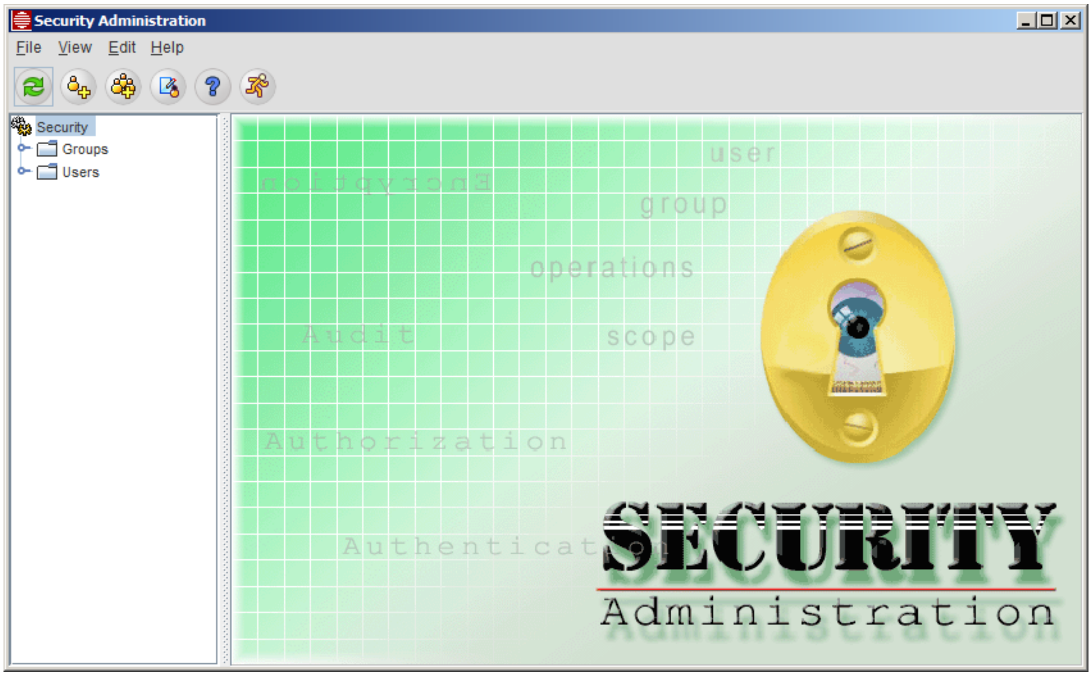


FIGURE 8-1 Security Administration – Main Display

You can perform the following tasks:

TABLE 8-1 Task List for Security Administration - User

Task	Screen / Form Name (if Applicable)	Section
Add User	User Wizard	"Adding a New User" on page 156
Configure User		
- Associate Groups	Select Groups	"Associating Groups to User" on page 159
- User Profile	User Profile Tab	"Setting the User Profile" on page 159
- Audit Trails	Audit Trails for User Tab	"Viewing Audit Trails" on page 161
- Change Password		"Changing the User Password" on page 162
- Assign Operations	Permitted Operations for User Tab	"Assigning Operations to User" on page 162
- Delete		"Delete User" on page 163
Add Group	Groups Wizard	"Adding a New Group" on page 163
Configure Group		
- Set Scope	Scope Settings	"Group and Scope Settings" on page 165
- Associate Users	Select Users Wizard	"Assigning Users to Group" on page 166
- Assign Operations	Operations Tree	"Assigning Operations to Group" on page 167
Custom View Scope (CVS)		
- Overview	Custom View Scope for Group Tab	"Custom View Scopes" on page 167
- Add Authorized Scope	Scope Settings	"Adding an Authorized Scope for a Custom View Scope" on page 167
- Set Authorized Scope for CVS	Select Authorized Scopes	"Setting an Authorized Scope for a Custom View Scope" on page 167
- Set Scope Properties	Scope Setting Wizard	"Setting Scope Properties" on page 168
- Delete Authorized Scope		"Deleting Authorized Scope" on page 169
Operations Tree		
- Overview, Add / Delete	Operation Tree Configuration	"Assigning Permissions" on page 169
- Default Operation Categories		"Permissions Tree Hierarchy" on page 170

TABLE 8-1 Task List for Security Administration - User (Continued)

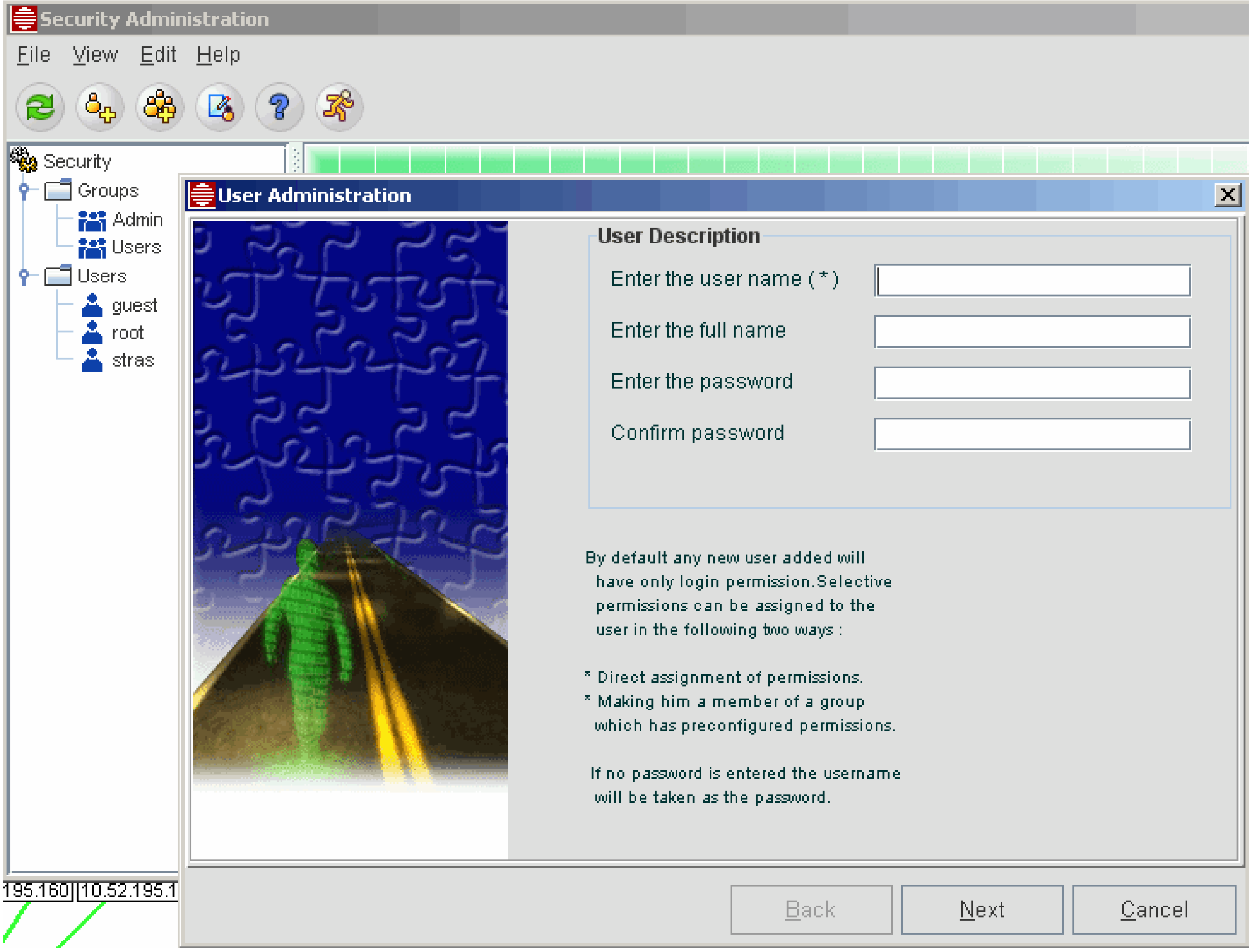
Task	Screen / Form Name (if Applicable)	Section
Remote Authorization (RADIUS / Tacacs+)		"Remote Authorization (RADIUS / Tacacs+) on Devices" on page 189
NMS RADIUS Client Support	RADIUS Configurator GUI	"NMS RADIUS Client Support" on page 192

8.2 Adding a New User

To add a new user do one of the following:

- Choose the **File** menu from the menu bar and select **New** under which you can select the option **AddUser**.
- Click the **Add User** icon in the Toolbar
- Right-click the node named **Users** in the left-side tree, which is a parent node.

The **User Administration** wizard appears.



User Description

Enter the user name (*)

Enter the full name

Enter the password

Confirm password

By default any new user added will have only login permission.Selective permissions can be assigned to the user in the following two ways :

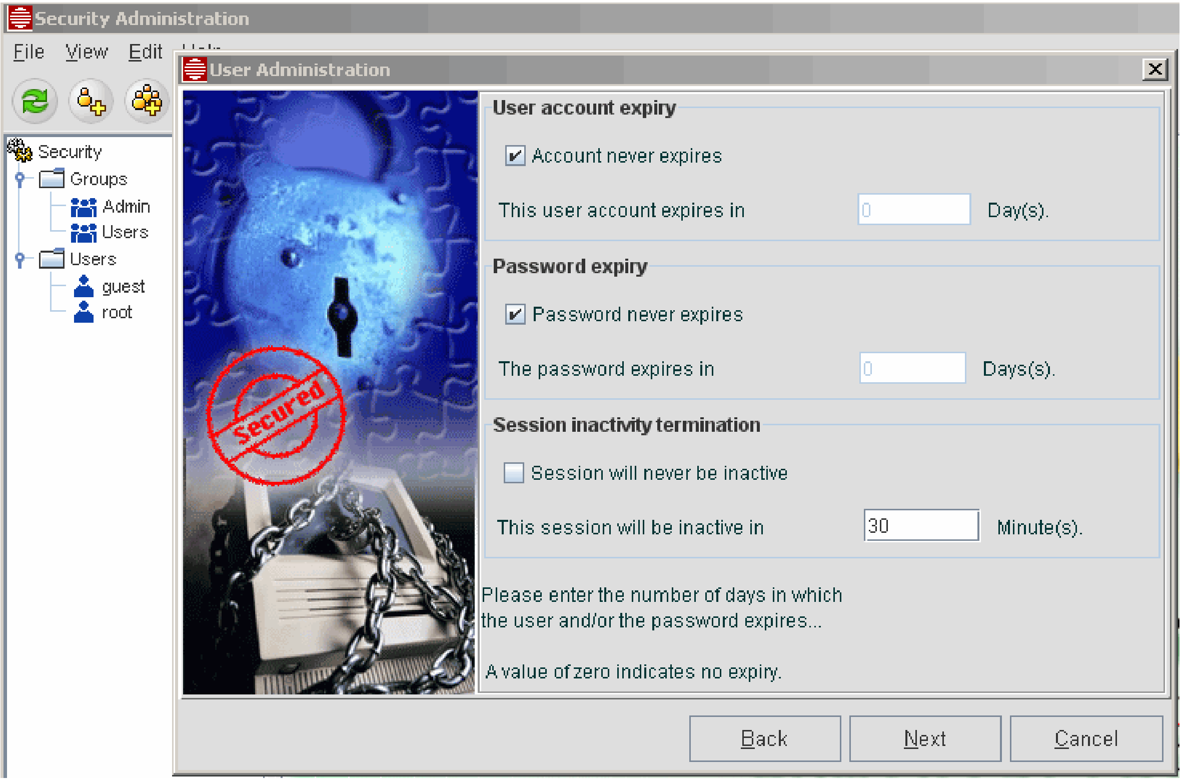
* Direct assignment of permissions.
* Making him a member of a group which has preconfigured permissions.

If no password is entered the username will be taken as the password.

FIGURE 8-2 User Administration Wizard (1)

Enter the username and password for the user in the corresponding text boxes. If no password is supplied, the username is also used as the password.

Click **Next** to move to the next screen, which is shown in the following figure.



User account expiry

☑ Account never expires

This user account expires in 0 Day(s).

Password expiry

☑ Password never expires

The password expires in 0 Days(s).

Session inactivity termination

□ Session will never be inactive

This session will be inactive in 30 Minute(s).

Please enter the number of days in which the user and/or the password expires...

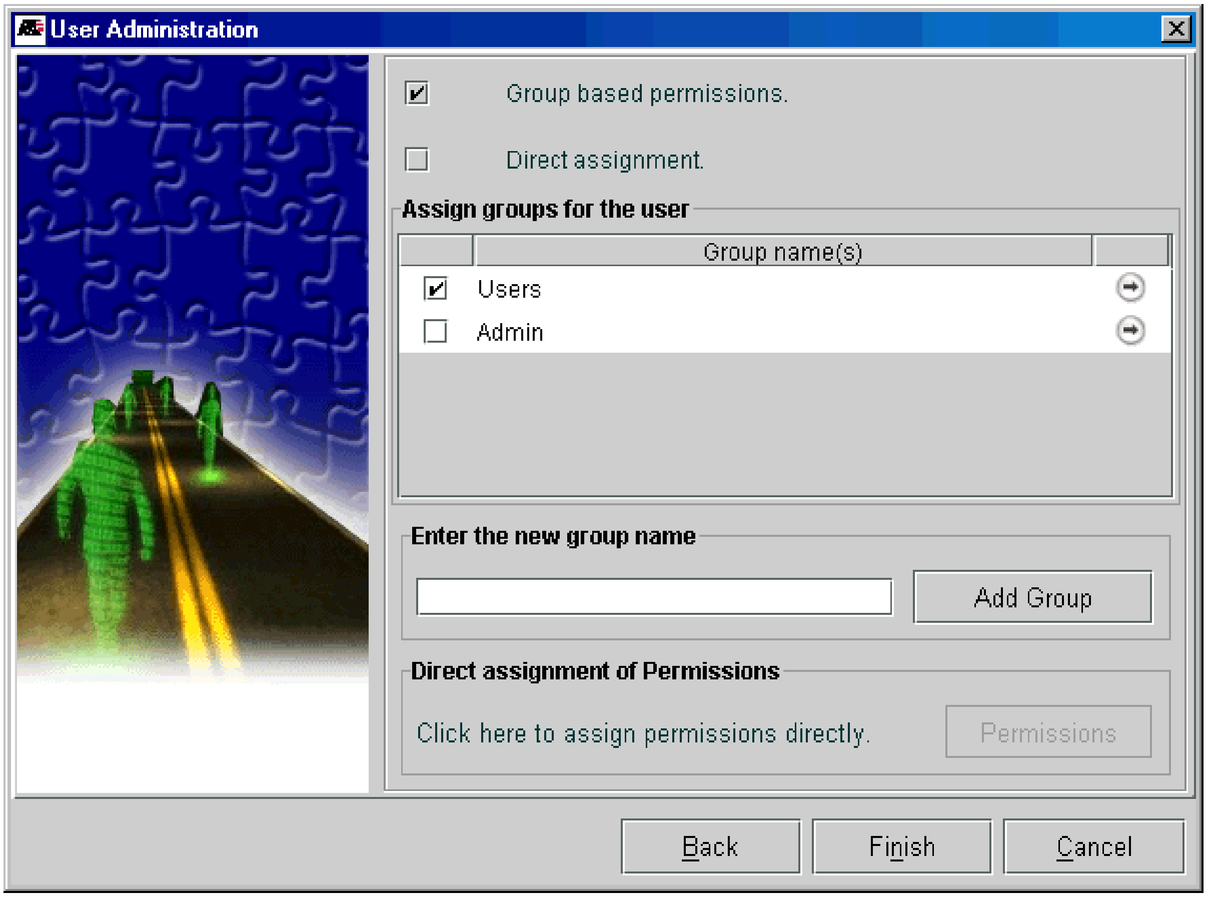
A value of zero indicates no expiry.

FIGURE 8-3 User Administration Wizard (2)

This **User Administration** screen shows the user account and password expiry in number of days. By default both values will be zero indicating that the user account and password never expire. If you need to set an expiry date for user account and password, uncheck the corresponding check boxes, and then enter the expiry period in the number of days.

The Session inactivity termination panel can activate the session timeout feature, by clicking on the Session Timer checkbox to make it not ticked (default is ticked), and then entering a value (in minutes).

After setting the user account expiry and password expiry time, the last screen of the User Administration Wizard, which is invoked by clicking **Next,** is where you can assign groups to the user or operations to the user directly. Refer to the following figure.



User Administration

☑ Group based permissions.

□ Direct assignment.

Assign groups for the user

	Group name(s)	
☑	Users	➡
□	Admin	➡

Enter the new group name

Direct assignment of Permissions

Click here to assign permissions directly.

FIGURE 8-4 User Administration Wizard (3)

Users can be associated with existing groups by clicking the appropriate check boxes of the groups when the checkbox **Group based permissions** is checked. You can also see the allocated operations for the existing groups by clicking on the right arrow for that group.

Note: *You can associate the new user to a new group by entering the new group name in the corresponding text box and clicking Add Group. The group is added and the operations for that group can be defined immediately. In most cases, however, a group should be defined first and then users associated with that group.*

To assign operations to the user directly without associating him or her with any groups, check **Direct assignment**. The **Permissions** button is activated, and the Administrator can assign operations to a user without associating them to any groups. Clicking **Permissions** will invoke the Permissions Tree Hierarchy. The Administrator can use this operations tree to allow/disallow operations for that user.

You can assign permissions by:

- Checking (checkmark) the check boxes to include the operations
- Ticking the check box (x) to exclude operations
- Leaving the check box empty so that it inherits its parent operation permission

Note: *Repeatedly clicking the checkbox will cycle the checkbox through these states (checkmark, x, empty).*

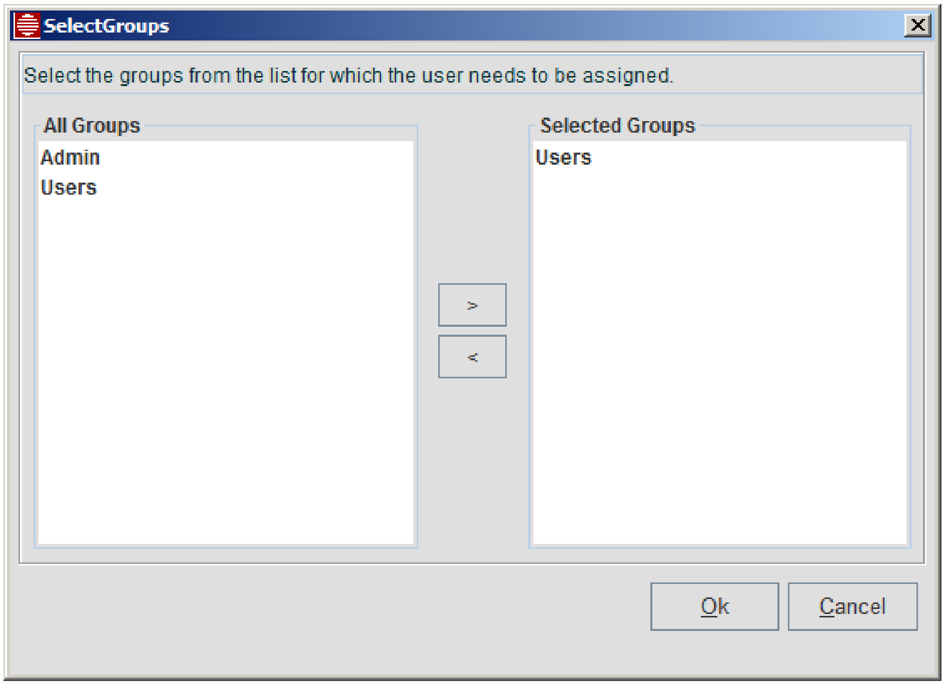
After associating groups to the new user, click **Finish** for confirmation. If you need to make any changes, you can go back to the previous screens by clicking **Back** and make the necessary changes. The new user added will be displayed under the left side tree under the parent node **Users** in the main **Security Administration** window.

8.3 User Settings

To perform user-level tasks, select the user in the left-side tree of the main **Security Administration** window under the parent node **Users**.

8.3.1 Associating Groups to User

After selecting the particular user, click **Setting Groups** in the lower right corner of the **Member Of** panel to associate the user with any of the existing groups or to remove the user from the already associated group, as shown in the following figure.



SelectGroups

Select the groups from the list for which the user needs to be assigned.

All Groups
Admin
Users

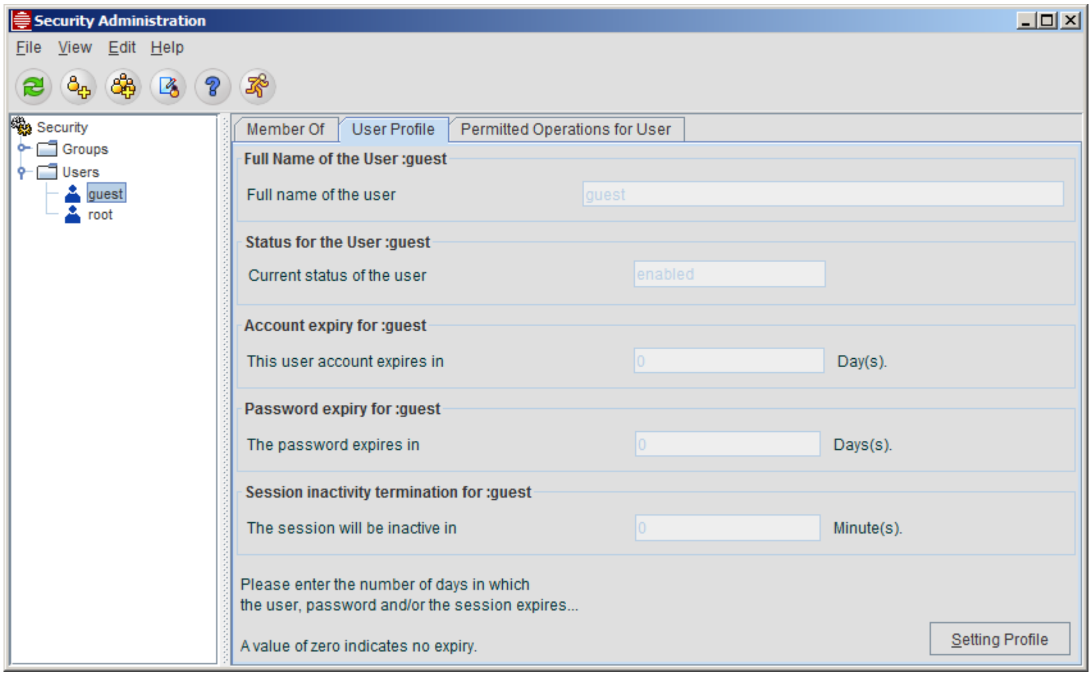
Selected Groups
Users

FIGURE 8-5 Associating Groups to User

In the left-side list are the existing groups and in the right-side list are the group names to which the user has already been associated. You can select the particular group from the left side and click the **>** (Add) button to associate the new group to the user. For removing the user from the already associated group, select the group in the right side from which the user needs to be removed and click the **<** (Remove) button.

8.3.2 Setting the User Profile

To modify user details, select the user, then select the **User Profile** tab to display the current user status, user account, password expiry in number of days, and the session inactivity termination for the user.



Full Name of the User :guest

Full name of the user: guest

Status for the User :guest

Current status of the user: enabled

Account expiry for :guest

This user account expires in 0 Day(s).

Password expiry for :guest

The password expires in 0 Days(s).

Session inactivity termination for :guest

The session will be inactive in 0 Minute(s).

Please enter the number of days in which the user, password and/or the session expires...

A value of zero indicates no expiry.

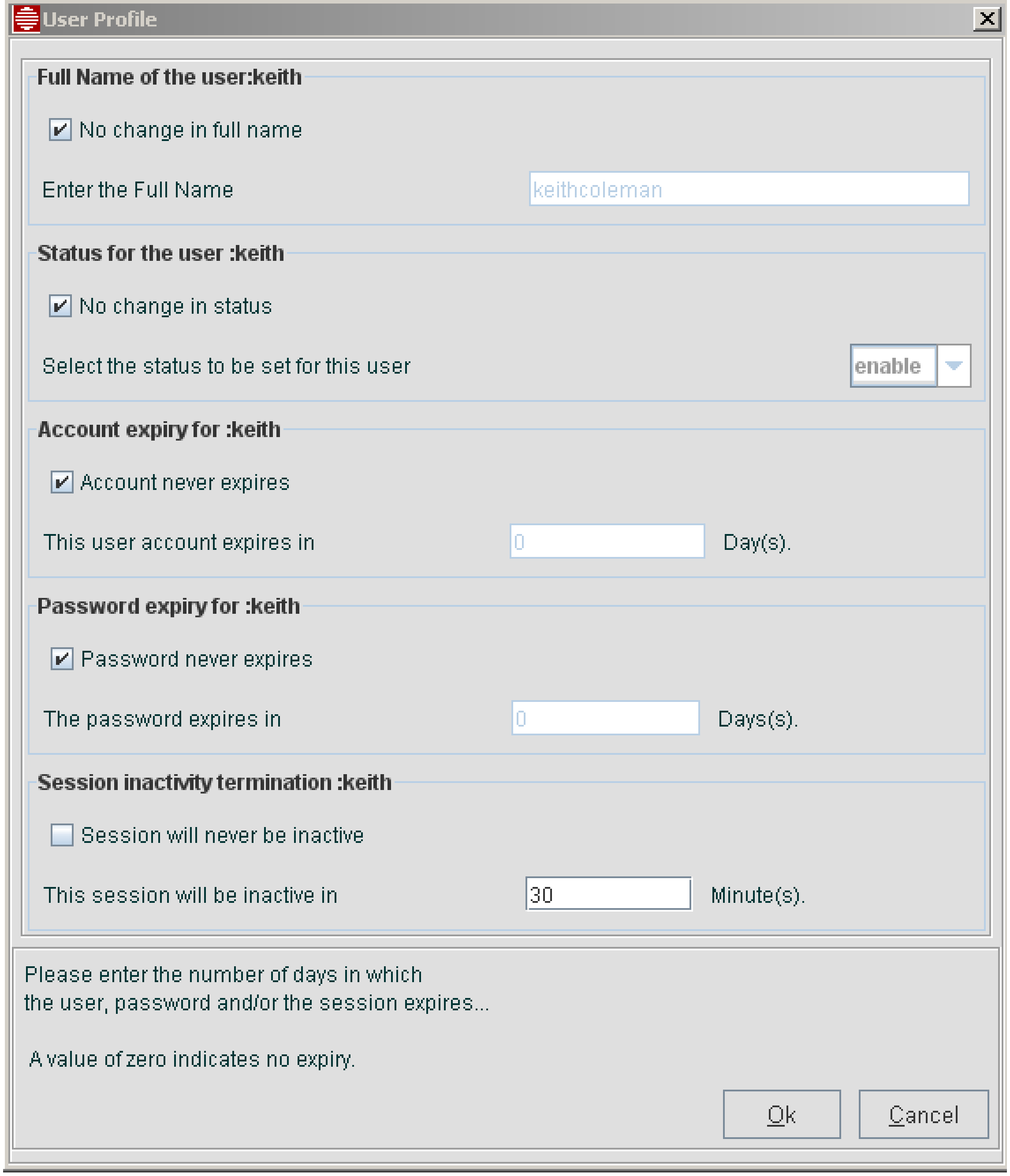
FIGURE 8-6 User Profile

The Security Administration tool displays each user’s current status using icons in the left-side tree under the **Users** node. Table 8-2 describes the user status icons.

TABLE 8-2 Icons for User Status

Icon	Description
👤	User Account is enabled
👤✖	User is disabled and he cannot login any more until he or she is enabled by the administrator
👤	User account has expired since the specified
🔑✖	User Password has been expired since the specified time and he or she has to change his password or reuse it
🖥👤	User account has been forced out from logging in to the server similar to the disable status of a user
👤✖	User's login has been denied due to continuous unsuccessful login attempts

Click **Setting Profile**, which will invoke the User Profile Wizard where you can set the user account expiry in days by clicking the corresponding check box. After the account expiry period, the status of the user is disabled and the user will not be allowed to log in on the network. Similarly, the user password expiry can be set in number of days, after which the user is prompted to enter a new password. Finally, you can change the session inactivity timer. You can also set the user status as either enable or disable by clicking the respective option. Refer to the following figure.



Full Name of the user:keith

☑ No change in full name

Enter the Full Name keithcoleman

Status for the user :keith

☑ No change in status

Select the status to be set for this user enable

Account expiry for :keith

☑ Account never expires

This user account expires in 0 Day(s).

Password expiry for :keith

☑ Password never expires

The password expires in 0 Days(s).

Session inactivity termination :keith

☐ Session will never be inactive

This session will be inactive in 30 Minute(s).

Please enter the number of days in which
the user, password and/or the session expires...

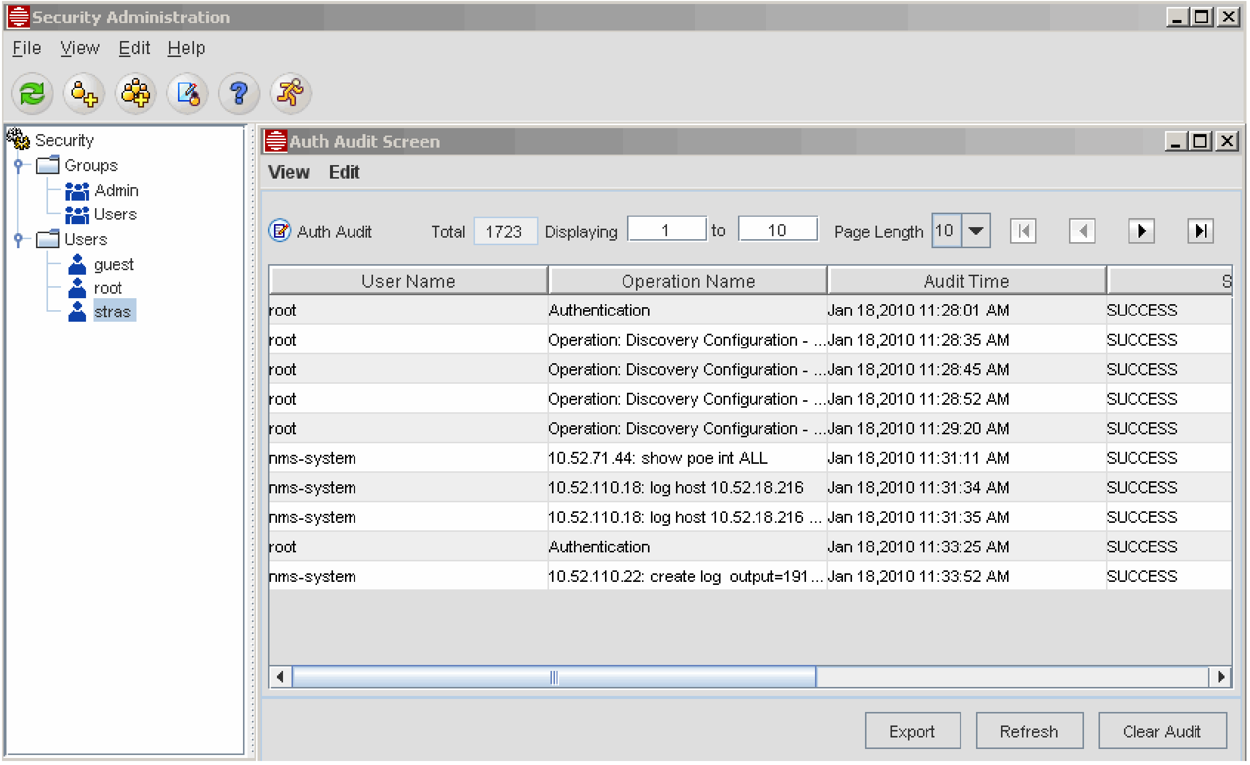
A value of zero indicates no expiry.

FIGURE 8-7 User Profile Wizard

After making the necessary changes click the **Ok** button for updating the server.

8.3.3 Viewing Audit Trails

The audit trails of all the users can be viewed by selecting the *View -> Audit Trails* menu or clicking the **Audit Trails** icon. This displays the **Audit Details** window where the various operations performed by the users along with the status whether the operation was a success or failure are displayed. Refer to the following figure.



Total 1723 Displaying 1 to 10 Page Length 10

User Name	Operation Name	Audit Time	S
root	Authentication	Jan 18,2010 11:28:01 AM	SUCCESS
root	Operation: Discovery Configuration - ...	Jan 18,2010 11:28:35 AM	SUCCESS
root	Operation: Discovery Configuration - ...	Jan 18,2010 11:28:45 AM	SUCCESS
root	Operation: Discovery Configuration - ...	Jan 18,2010 11:28:52 AM	SUCCESS
root	Operation: Discovery Configuration - ...	Jan 18,2010 11:29:20 AM	SUCCESS
nms-system	10.52.71.44: show poe int ALL	Jan 18,2010 11:31:11 AM	SUCCESS
nms-system	10.52.110.18: log host 10.52.18.216	Jan 18,2010 11:31:34 AM	SUCCESS
nms-system	10.52.110.18: log host 10.52.18.216 ...	Jan 18,2010 11:31:35 AM	SUCCESS
root	Authentication	Jan 18,2010 11:33:25 AM	SUCCESS
nms-system	10.52.110.22: create log output=191...	Jan 18,2010 11:33:52 AM	SUCCESS

FIGURE 8-8 Audit Trail Details - File

You can save the audit details in a file for future reference to identify any access violation. To clear all the previous audit details, click **Clear Trails**.

Note: Actions such as command input for a device can also be recorded by the SYSLOG application; the benefit of the Audit is that it shows commands that were invoked using the NMS as well as the user who invoked the command.

8.3.4 Changing the User Password

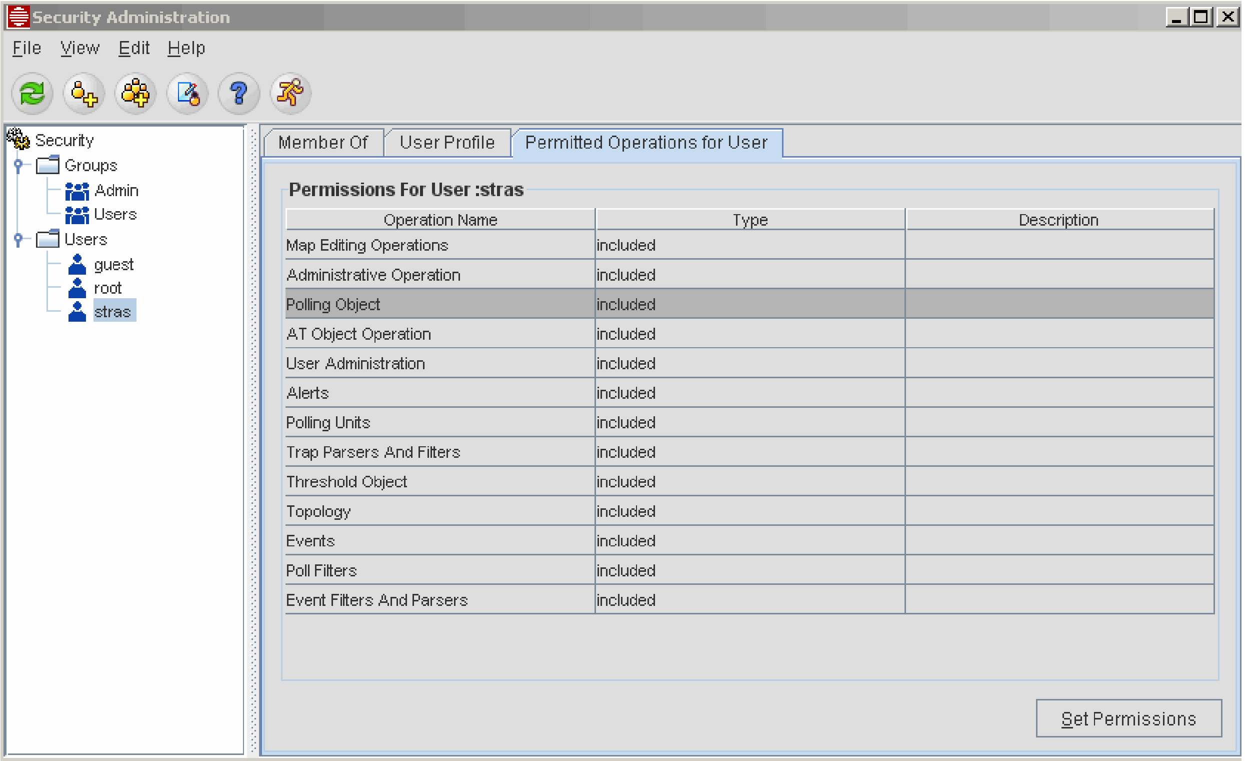
To change a user's password:

For a selected user you can change the password by right-clicking and selecting the *Change Password* option from the pop-up menu, or by selecting *Edit -> Change Password* from the menu of the **Security Administration** window.

This displays the **Change Password** window, which has text boxes in which the new password can be entered and confirmed. After entering the new password and confirming it, click **OK** for the respective change.

8.3.5 Assigning Operations to User

Click the **Permitted Operations for User** tab after selecting the particular user for whom you want to assign operations. This shows the already included and excluded operations for the respective user. In order to assign new operations, click **Set Permissions**. This invokes the operations tree as shown in the following figure.



Permissions For User :stras

Operation Name	Type	Description
Map Editing Operations	included	
Administrative Operation	included	
Polling Object	included	
AT Object Operation	included	
User Administration	included	
Alerts	included	
Polling Units	included	
Trap Parsers And Filters	included	
Threshold Object	included	
Topology	included	
Events	included	
Poll Filters	included	
Event Filters And Parsers	included	

FIGURE 8-9 Permission Tree Hierarchy

The operations tree is a union of the operations included or excluded of the groups and the directly assigned operations. Thus you can assign permissions to the operations that are not associated with the group for the user. In order to modify the permissions set to the user through groups, go to the **Permitted Operations For Group** tab after selecting the particular group, and then click **Set Permissions** to do the necessary changes. In the operations tree, by clicking the respective check boxes of the operations, you can include that operation for the user, and by ticking the check box (x), you can exclude that respective operation for the user. After making the necessary selections click **Done** to make the change permanent.

You can assign permissions by:

- Checking (checkmark) the check boxes to include the operations
- Ticking the check box (x) to exclude operations
- Leaving the check box empty so that it inherits its parent operation permission.

8.3.6 Delete User

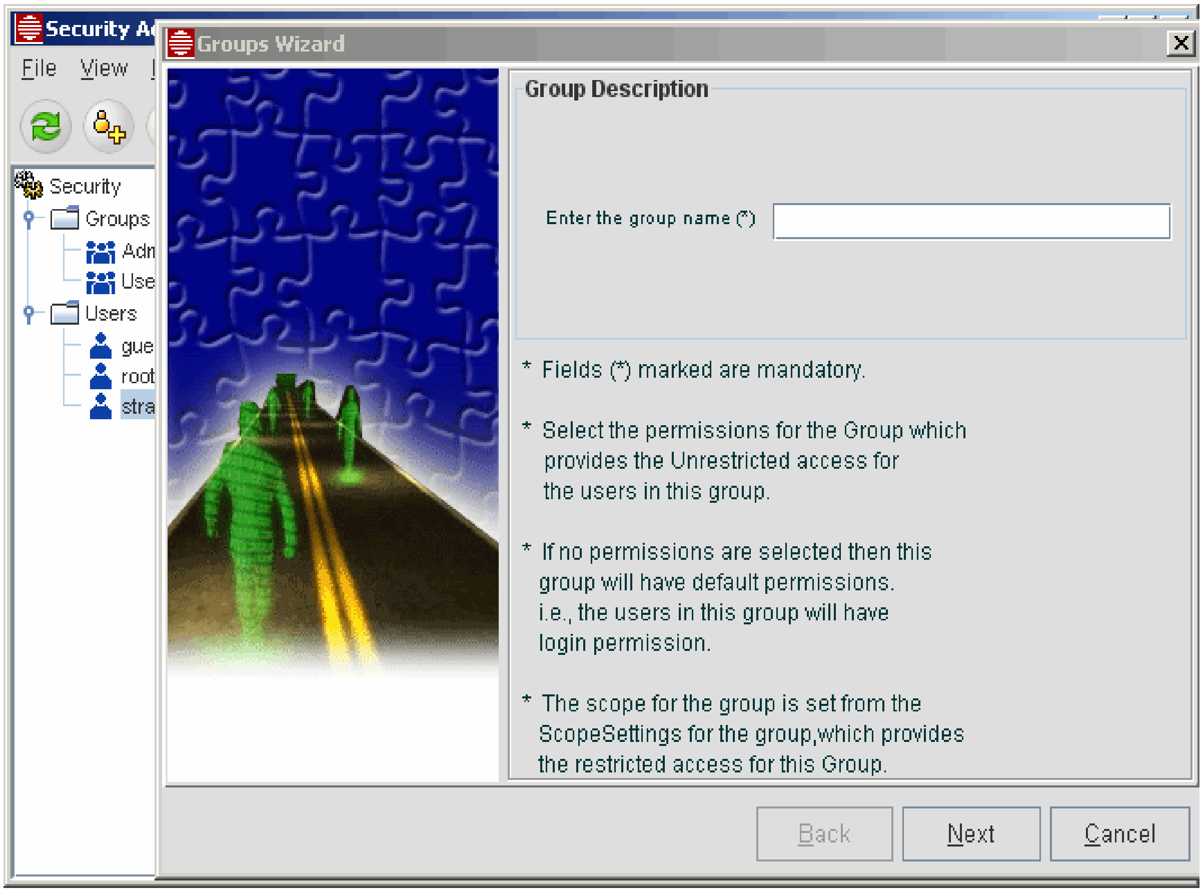
To delete a user, right-click the user and select *Delete* from the pop-up menu, or select *Edit -> Delete* option from the menu of the **Security Administration** window. This deletes the user and all his or her associated operations and groups.

8.4 Adding a New Group

In the **Security Administration** window, you can add a new group by performing one of the following actions:

- Select *File -> New -> AddGroup* from the menu bar.
- Click the **Add Group** icon from the Toolbar.
- Right-click the node **Groups** in the left-side tree, which is a parent node.

Each of these actions invokes the **Groups wizard**, shown in the following figure, where you can enter the new group name in the text box.



Group Description

Enter the group name (*)

* Fields (*) marked are mandatory.

* Select the permissions for the Group which provides the Unrestricted access for the users in this group.

* If no permissions are selected then this group will have default permissions. i.e., the users in this group will have login permission.

* The scope for the group is set from the ScopeSettings for the group,which provides the restricted access for this Group.

FIGURE 8-10 Groups Wizard (1)

After entering the group name, click **Next,** which invokes the second screen of the Groups Wizard, as shown in the following figure.

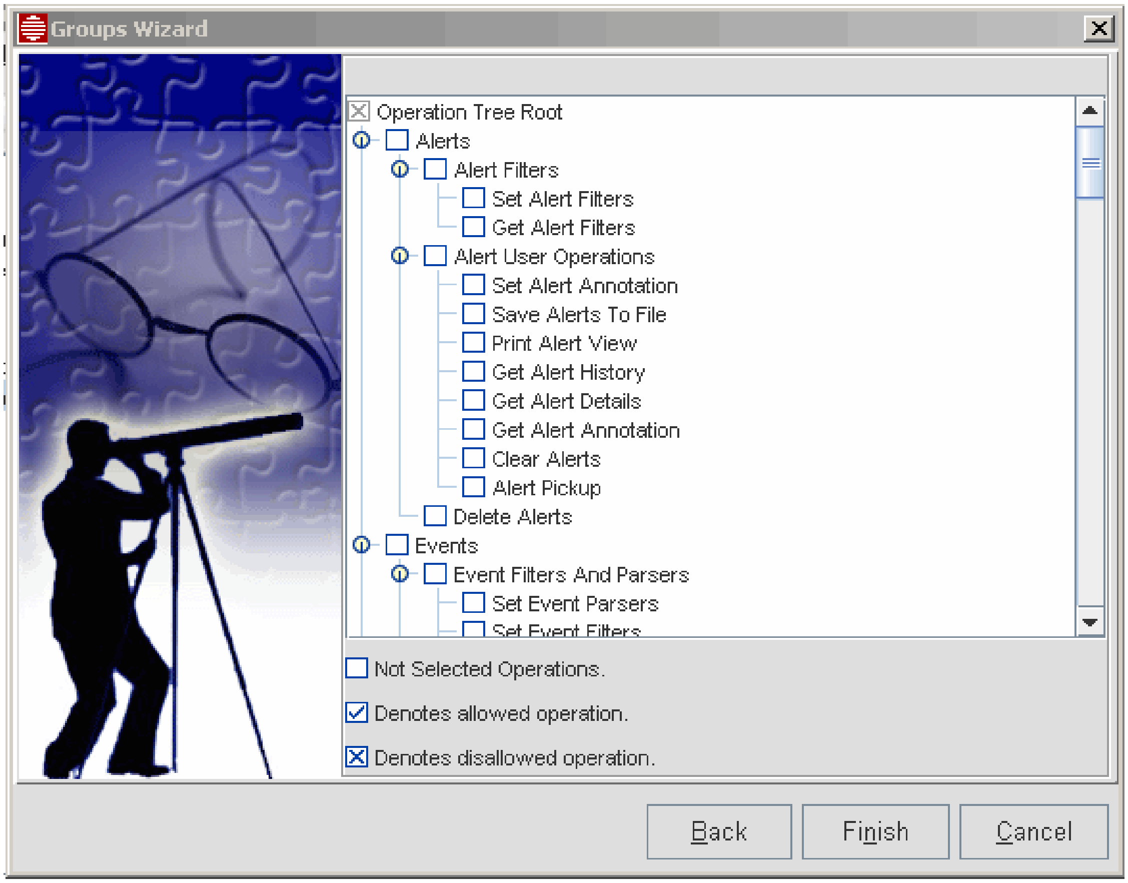


FIGURE 8-11 Groups Wizard (2)

You can assign operations for the group by:

- Selecting (checkmark) the check boxes to include the operations
- Ticking the check box (x) to exclude operations
- Leaving the check box empty so that it inherits its parent operation permission.

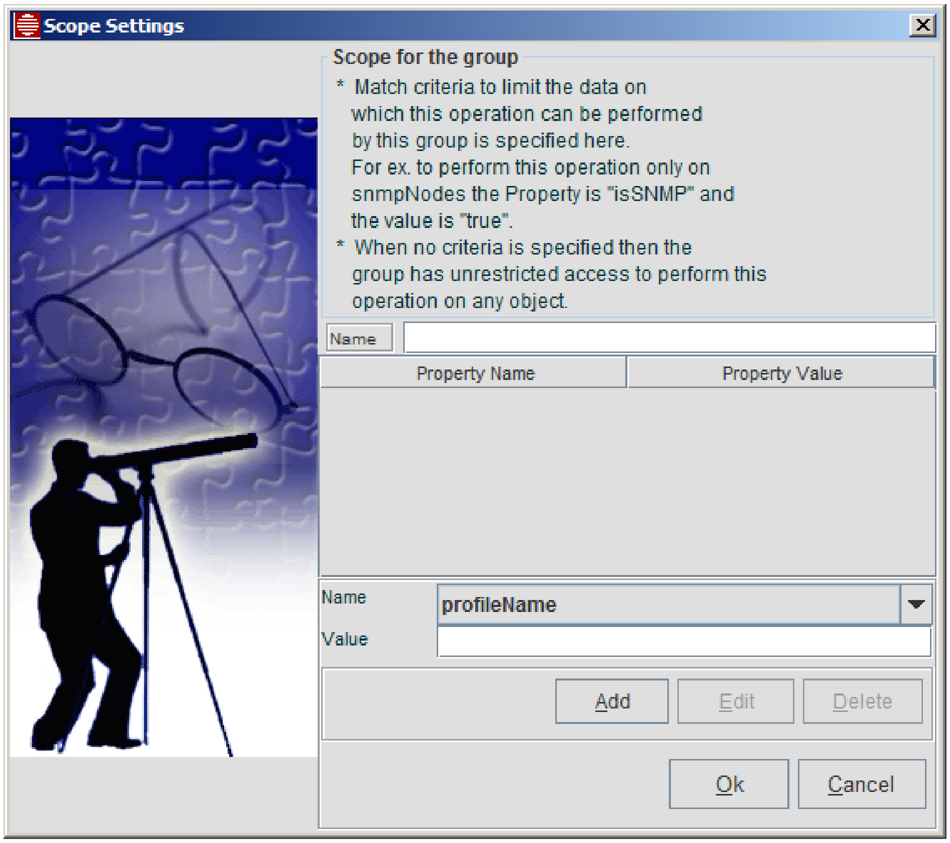
After selecting the operations, click **Finish** to save the changes permanently in the server.

8.4.1 Group and Scope Settings

Authorized Scopes (or Authorized Views) are independent entities that store the real authorization information. The scopes are associated with the actual operations of the group leading to a more specific authorization for the user. Scopes consists of a set of properties, and the scope is applicable only when those properties are true. For example, if you give a property as network=192.168.4.0, the scope of that associated operation is applicable only for this network. The Scopes associated to the respective operations are grouped together under the groups and then allocated to the users. The Administrator can perform the following tasks under Scope configuration.

8.4.1.1 Add a Scope

Select a particular group for which you want to set a scope for the operations under that group, and then select the **Permitted Operations for Group** tab in the **Security Administration** window. Now select the operation for which you wish to set a new scope, and then click **Setting Scope**. This invokes the Scopes Settings Wizard, which helps in adding a new scope, as shown in the following figure.



* Match criteria to limit the data on which this operation can be performed by this group is specified here. For ex. to perform this operation only on snmpNodes the Property is "isSNMP" and the value is "true".
* When no criteria is specified then the group has unrestricted access to perform this operation on any object.

Name:

Property Name	Property Value

Name: profileName
Value:

FIGURE 8-12 Scope Settings

To add a new scope, perform the following:

- Give the property name and property value for the selected operation scope.
- Click **Add** in the wizard.
- Click **Ok** to save the changes and to exit.

8.4.1.2 Edit a Scope

To edit a scope, select it and click **Edit**. The inputs given for the respective operation's scope that can be edited are Property Name and Property Value.

8.4.1.3 Delete a Scope

To delete a scope, select the respective Property row of the scope to be deleted, and then click **Delete**.

Note: Scopes can be configured to Operations of Groups with properties. The Administrators can add a list of scope to a single operation or more of the groups and then assign the group to the users. Properties are then added for more specific authorization.

8.4.2 Assigning Users to Group

Users can be assigned to the group by selecting the particular group from the left side of the **Security Administration** window under the parent node **Groups** and in the **Members** tab screen in the right, click **Setting Users**. This invokes the Select Users Wizard where you can see all the user names in the left-side column and the selected users for the particular group in the right-side column. Between these two columns are the **Add** and **Remove** buttons by which you can select a particular user and either add the user to the group or remove the user from the group.

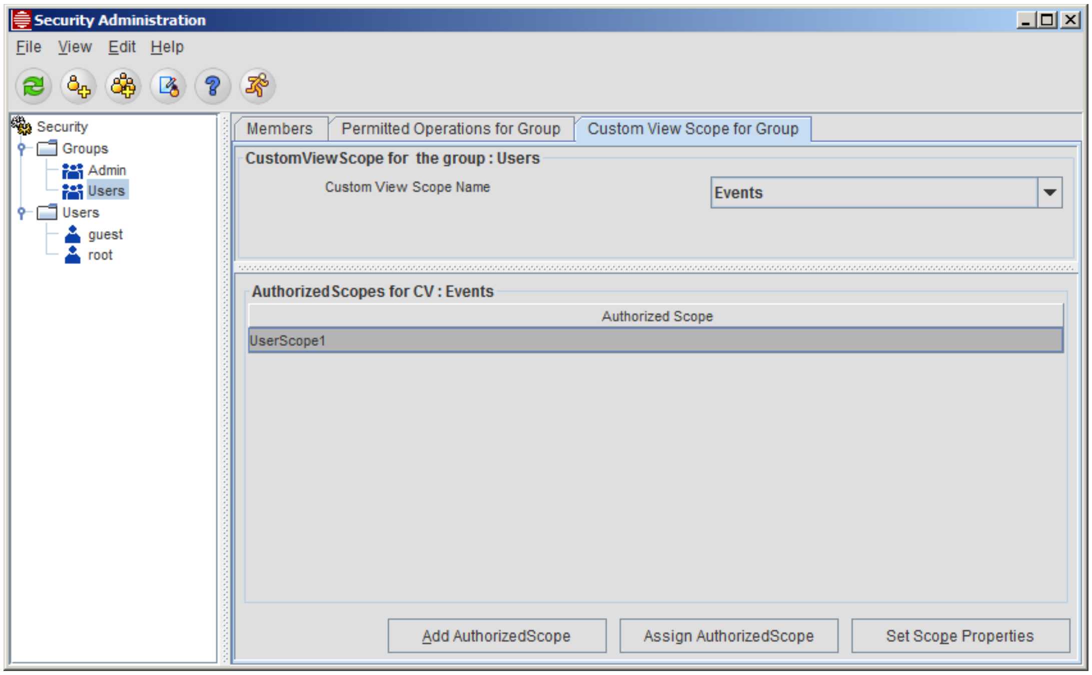
8.4.3 Assigning Operations to Group

To assign operations to the group, select the particular group and click the **Permitted Operations for Group** tab in which you can click **Set Permissions**. This invokes the operation tree where you can allow or disallow operations for that group by clicking the check boxes of the respective operations, and then clicking **Done** to make the changes permanently in the server and to exit the operations tree. Thus, the tasks under the Group Settings are performed.

8.5 Custom View Scopes

As the administrator, you can set custom view scopes to filter which objects display in the NMS for groups of users. When you specify custom view scope criteria for groups of users, users in those groups can view only those objects that they are authorized to operate.

To add or edit custom view scopes, use the **Custom View Scope for Group** tab, displayed in Figure 8-13.



CustomViewScope for the group : Users

Custom View Scope Name: Events

AuthorizedScopes for CV : Events

Authorized Scope
UserScope1

FIGURE 8-13 Custom Scope View

Following are the list of tasks that can be done for the selected Custom View Scope of a group.

8.5.1 Adding an Authorized Scope for a Custom View Scope

Custom view scopes are added through the group and scope settings. To add an authorized scope to the available Custom View Scope of the group, select the relevant Custom View Scope Name and click **Add AuthorizedScope,** which will invoke the **Scope Settings** form.

In the **Scope Settings** form**,** enter the Authorized Scope Name in the respective text box, and then enter the required Name and Value for the property of the scope. The Administrator can give more than one value as comma-separated property values for a property name. Now, click **Add,** which adds the Authorized Scope for the selected Custom View Scope of the group, and then click **Ok** to make the change permanent.

8.5.2 Setting an Authorized Scope for a Custom View Scope

In order to set Authorized Scope for the selected Custom View Scope of the group, click **Set AuthorizedScope**. This will invoke the **Select AuthorizedScopes** screen, in which the left-side column displays all the AuthorizedScopes set for the operations of the groups, which are already present, and the right-side column displays the previously set Authorized Scopes or the selected Custom View Scope name. Thus, you can select the respective scope to be set for the custom view in the left and click **>** (Add). To remove the already existing authorized scope set for the Custom View, select the respective scope in the right side column, and click **<** (Remove) button. Click **OK** to save the changes permanently in the server.

Scope changes take effect the next time a user logs in. Users in multiple groups will see the scope with the most restricted settings of all the groups to which they are assigned.

8.5.3 Setting Scope Properties

To set properties to the Authorized Scopes of the Custom View Scope, select the respective row of the Authorized Scope and click **Set Scope Properties** to open the **Scope Settings** box, where you can set properties for the selected Authorized Scope.

The naming convention for cards is:

<host>_<slot>

The naming convention for interfaces is:

<host>_<slot>.<port>

Table 8-3 describes the wild card characters available to specify scope criteria values.

TABLE 8-3 Operators for Setting Scope Criteria

Operator	Description
* (Asterisk)	This is used to match zero or more characters. *Example*: If the names of all the objects starting with the name "test" is needed, then the property Name - **name** and the Value **test*** is given.
! (Exclamation Mark)	This is used for filtering the search using NOT operator. *Example*: If all the objects whose name does not start with "test" is required, then property key - **name** and value - **!test*** is given.
, (Comma)	This is used for searching objects where a single property key has different values. *Example*: If all the objects with names starting with "abc" or "xyz" are required, then property key - **name** and value "**abc*,xyz***"is given
&&	This is also used for searching objects where a single value should be matched with many patterns. *Example:* If all the objects with names starting with either "abc" and ending with "xyz" are required, then property key -**name** and value "**abc*&&*xyz**" is given.
\ (Back Slash)	This is used when the name of the object itself contains a comma. This character is called an escape sequence, since it avoids searching of the objects, as if it were two different names. *Example:* If an object with name "a, b" has to be searched, then the property key - **name** and the value - "**a\, b**" is given. <between>"value1" and "value2" This is used to get objects with some numeric values within a specific range.
<between>"value1" and "value2"	This is used to get objects with some numeric values within a specific range. Example: If object names with poll interval values ranging from 300 to 305 are required, then the property key - **pollinterval** and the value as **300** and **305** is given. Note that the first number is smaller than the second number. Only the values between the given values, including the limits, will be matched.

To determine what custom view scope properties are available, see "Object Properties to Define Objects and Custom Views" on page 1051.

Scope criteria values are limited to 50 characters. If your criteria exceed 50 characters, you must set up separate custom view scopes. For example, instead of creating a single view scope to display multiple cards on an iMAP device, you can create a view scope for each card. See "Extending the Two Service Provider Example" on page 202 for additional examples.

8.5.4 Deleting Authorized Scope

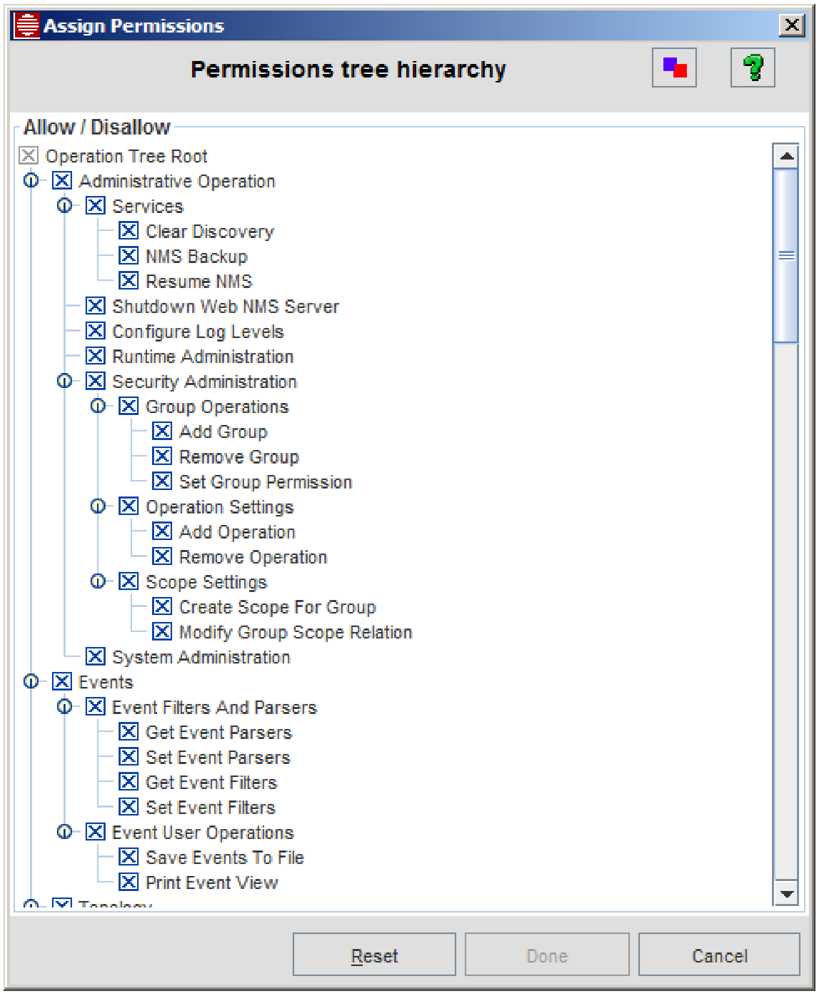
The Authorized Scopes associated to a Custom View Scope can be deleted completely from the database by right-clicking the respective Authorized Scope, and then clicking the pop-up button **Delete AuthorizedView**. This will display a warning dialog box. Click **Yes** in the dialog box to delete the view scope.

Deleting the selected Authorized Scope of the respective Custom View Scope will remove it completely, not only from the current selected group, but also from the other associated groups. Hence, in order to delete an Authorized Scope set for a Custom View Scope only from the selected group, click **Assign Authorized Scope** and dissociate it from the current selected group.

8.6 Assigning Permissions

The NMS operations are logically arranged in a tree structure, with parent and child operations in the tree. This tree is displayed when assigning permissions to a group or a user. The tree is referred to as the Permissions Tree and is shown in Figure 8-14. Permission to perform individual operations can be granted or denied for each group or user through this tree.

Note: The tree node AT Object Operations includes those operations that the NMS can perform on Allied Telesis devices.



Allow / Disallow

- ☒ Operation Tree Root
- ☒ Administrative Operation
  - ☒ Services
    - ☒ Clear Discovery
    - ☒ NMS Backup
    - ☒ Resume NMS
  - ☒ Shutdown Web NMS Server
  - ☒ Configure Log Levels
  - ☒ Runtime Administration
  - ☒ Security Administration
    - ☒ Group Operations
      - ☒ Add Group
      - ☒ Remove Group
      - ☒ Set Group Permission
    - ☒ Operation Settings
      - ☒ Add Operation
      - ☒ Remove Operation
    - ☒ Scope Settings
      - ☒ Create Scope For Group
      - ☒ Modify Group Scope Relation
  - ☒ System Administration
- ☒ Events
  - ☒ Event Filters And Parsers
    - ☒ Get Event Parsers
    - ☒ Set Event Parsers
    - ☒ Get Event Filters
    - ☒ Set Event Filters
  - ☒ Event User Operations
    - ☒ Save Events To File
    - ☒ Print Event View
- ☒ Topology

FIGURE 8-14 Permissions Tree Hierarchy

8.6.1 Permissions Tree Hierarchy

The Permissions Tree Hierarchy contains a list of operations that are provided by default in the NMS. Assigning different operations to different users is an administrative function. The different operations that can be assigned are explained in the following tables.

8.6.1.1 Administrative Operations

TABLE 8-4 Administration Operations

Operation	Description
Services	
Clear Discovery	This operation is used when the Discovery process has stopped.
NMS Backup	This Operation starts the backup process by setting BackUpInProcess variable to true and suspends all NMS Schedulers. Once the backup process is over, automatically resets the BackUpInProcess variable to false, to resume NMS Schedulers.
Resume NMS	This Operation can be used to resume all the NMS Schedulers, if NMS hangs due to some unforeseen problems during the backup process.
Shutdown server	This Operation is used for shutting down the NMS Server with authentication.
Configure Log Events	This Operation provides the link to view the present logging levels for the various modules. The logging also can be set by using this Operation.
Security Administration	Security Management involves work starting from authenticating a user when logging till dictating all permissions for him and thus defining the access limits for every user.
System Administration	This Operation is for getting the handle for all the Administrative Operations.

8.6.1.2 Events

Network Events are entities that represent the various happenings in the network devices. Events can either convey any general information or the current status of the devices in a network. The groups of operations which are grouped under Events are listed in the table given below.

TABLE 8-5 Operations for Events

Operation	Description
Event Filters and Parsers	
Get Event Parsers	This Operation is for viewing the Event Parsers present in the server.
Set Event Parsers	This Operation is for modifying the existing Event Parser or creating a new Event Parser.
Get Event Filters	This Operation is for viewing the Event Filters present in the server.
Set Event Filters	This Operation is for modifying the existing Event Filter or creating a new Event Filter.
Event User Operations	
Save Events to File	This Operation is for saving the events displayed either in Events Panel or the selected events.
Print Event View	This Operation is for printing either the selected events or events displayed in the Events Panel.

8.6.1.3 Topology

Topology is used to add, update, delete and filter out the core Managed Objects from the database. The various operations grouped under the topology module are listed in the table given below. All are under Modify Object.

TABLE 8-6 Operations for Topology

Operation	Description
Start and Stop Discovery	This Operation is used to set the discovery status for the particular Object.
Manage and Unmanage Objects	This Operation is used to set the management status of the particular Object.
Add Network	This Operation is used to add a new network in the Topology database.
Add Node	This Operation is for adding a new node in the Topology database.
Delete Object	This Operation is for removing a particular Object from the Topology database.
Refresh Node	This Operation is for updating the status polling.

8.6.1.4 User Administration

This Operation family is mainly used in HTML UI for User Administration. The various operations available by default under User Administration are listed below.

TABLE 8-7

Operation	Description
User Configuration	This Operation is used to get the link for 'User Administration'.
Add Users	This Operation is used to create a new user.
Assign User to Group	This Operation is used to assign the user to new or existing group.
Remove User	This Operation is used to remove the user from the group.
Remove User from Group	This Operation is used to remove the particular user from the particular group only.
Get List of Users	This Operation is used to view the list of users present in the database.

8.6.1.5 Trap Parsers and filters

The various operations grouped under Trap Parsers and Filters are listed in the table given below.

TABLE 8-8 Operations for Trap Parsers and Filters

Operation	Description
Get Trap Filters	This Operation is for viewing the Trap Filters present in the server.
Set Trap Filters	This Operation is for modifying the existing Trap Filter or creating a new. Trap Filter.
Reload Trap Filters	This Operation is used to update the changes of the filter, without restarting the Server.
Get Trap Parsers	This Operation is for viewing the Trap Parsers present in the server.
Set Trap Parsers	This Operation is for modifying the existing Trap Parser or creating a new Trap Parser.

8.6.1.6 Alerts

Alerts are generated when a failure or fault is detected in the network devices. The generated Alerts get displayed in the Alert Viewer. The Alert list containing alarms of various severities like critical, major, minor, clear etc. can be viewed in the Alert Viewer. The various operations available by default under User Administration are listed below.

TABLE 8-9 Operations for User Administration

Operation	Description
Alert Filters	
Get Alert Filters	Operation is for viewing the Alert Filters present in the Server.
Set Alert Filters	This Operation is for modifying the existing Alert Filter or creating a new Alert Filter.
Set Alert Annotation	This Operation is for adding notes (annotation) to an alert.
Alert User Operations	
Get Alert Details	This Operation is for viewing the details of a particular alert.
Save Alerts to File	This Operation is for saving either the selected alerts or the alerts displayed in the current Alert Panel into a file.
Print Alert View	This Operation is for printing either the selected alerts or the alerts displayed in the current Alert Panel.
Clear Alerts	This Operation is for changing the Alert Severity as Clear.
Get Alert Annotation	This Operation is for viewing the particular existing alert annotation.
Get Alert History	This Operation is for viewing the Alert History, i.e., the change in status of an Alert from the first Alert to the latest Alert.
Alert Pickup	This Operation is used to pick up the Alert. (To attach one's ID to an alert so others know the alert is being worked.)
Delete Alerts	This operation is used to remove a particular alarm (usually because it has been solved).

8.6.1.7 Maps

A map is a graphical representation of networks and systems. Elements such as computer devices, printers, switches etc. connected in a network can be represented in a map. The operations available under Maps are listed below.

TABLE 8-10 Operations for Maps

Operation	Description
Map Editing Operations	This Operation is mainly used to configure the maps, like creation of new maps, customizing of map hierarchy, map symbol layout and map symbol renderers through the client.

8.6.1.8 Polling Unit

Polling units mentioned here refer to PolledData objects which are the basic unit of data collection. These define what data to be collected and from which network device. PolledData can be added via Client User interface. The operations possible with PolledData objects are listed below.

TABLE 8-11 Operations for Polling Units

Operation	Description
Add Polling Units	This operation permits you to add new PolledData to devices, to collect data for particular Data identifiers.
Remove Polling Units	This operation permits you to modify the definition of PolledData to change Data collection configuration.

TABLE 8-11 Operations for Polling Units

Operation	Description
Modify Polling Units	This operation permits you to remove the PolledData objects from database so that no more data is collected for the associated Data identifier.
Get Polling Unit	Get Polling Unit This operation permits you to retrieve PolledData details from database. If this operation is excluded in Operations Tree, you will not be able to see the PolledData information in StatsAdminPanel of Client UI.

8.6.1.9 Polling Objects

This object contains information on data collection configuration like match criteria and data to poll. Match criteria indicates from which devices data have to be collected and data to poll indicates what data to Polling objects can be created via Client User Interface, configuration file i.e. Polling.conf and API methods. The different operations possible with Polling objects are listed below.

TABLE 8-12 Operations for Polling Objects

Operation	Description
Add Polling Object	This Operation is used to create a new Polling Object and add to database for monitoring a new device or the existing device.
Delete Polling Object	This Operation is used to remove the existing Polling Objects.
Modify Polling Object	This Operation is used to modify the criteria of the existing Polling Object for making performance analysis better.
Change Polling Object Status	The Polling Object can be enabled or disabled by using the optional parameters called “status”. The parameter can be changed as “True” or “False”. The Operation 'Change Polling Object Status' is used to change the status of the polling Object.
Get Polling Object	This Operation is used to view the criteria of the particular Polling Object.

8.6.1.10 Poll Filters

Poll Filter is used to fine tune the Data collection configuration. When NMS Server starts Managed objects are created and they are passed through Polling.conf. If match criteria satisfies, according to the definition of Polling object, PolledData are created. Just before these PolledData objects are added to database, existing PolledData can be modified, new PolledData can be added for the Managed object or existing PolledData can be removed using Poll Filters. Different operations possible with Poll Filters are listed in the following table.

TABLE 8-13 Operations for Poll Filters

Operation	Description
Get Poll Filters	This operation permits retrieval of Poll Filters from the database and display them. If excluded will not allow you to view the Poll Filters list.
Update Poll Filters	This operation permits to modify Poll Filter related details.
Reload Poll Filters	This operation permits reloading to memory the modified Poll filter definitions specified in Poll filters file.

8.6.1.11 Threshold Objects

Thresholds are the basic unit for generating Threshold Events. Threshold Events are those events which get generated when the collected value for a particular agent satisfies the threshold criteria. The Threshold objects are formed by reading the Threshold.conf present in <NMS Home>/conf directory, which contains information about the thresholds that has to be generated when a particular condition is satisfied. The various default operations possible with Threshold Objects are provided in the following table.

TABLE 8-14 Operations for Threshold Objects

Operation	Description
Add Threshold Object	This Operation is used to create a new Threshold Object to create Threshold Events for a new device or the existing device.
Modify Threshold Object	This Operation is used to modify the existing Threshold Object for making performance analysis better.
Delete Threshold Object	This Operation is used to remove the existing Threshold Object.
Get Threshold Object	This Operation is used to view the particular Threshold Object.

8.6.1.12 AT Object Operation

AT Object Operation contains operations specific to Allied Telesis products. These operations are provided in the following table.

TABLE 8-15 Operations for AT Object Operation

Operation	Description
Performance Operation	
Monitor Collections Operations	Permits the Monitored Collections dialog for routers
Statistics Operation	Permits the Performance/Configured Collections display
Configuration Operation	
Configure SNMP Operation	Permits Configured SNMP MDTI operation
Device Backup/Restore Operation	Permits backup and restore operations
Software Configuration Operation	Permits software configuration operations
Device Information Operation	Permits the display of device information
SNMP Agent Operation	Permits SNMP Agent operations
SNMP Community Operation	Permits SNMP Community operations
Configure VLAN Operation	Permits VLAN configuration operations (Includes EPSR)
Card Management Operation	Permits card management operations
Port View Operation	Port Management Operation (complete control) Port Provision Operation (view and provision/deprovision)
SysLog Management Operation	Permits access to syslog application
Command Script Mgmt Operation	Permits command script management operations

TABLE 8-15 Operations for AT Object Operation

Operation	Description
Configuration File Mgmt Operation	Permits file management operations
Profile and QoS Operation	Profile and QoS Policy Operations
Rediscover Operation	Permits rediscovery operations
Application Manager Operation	Permits access to the Application Manager
Telnet Cutthru Operation	Permits Telnet cut-through
GUI Cutthru Operation	Permits GUI cut-through
Manage CLI Users Operation	Permits CLI user management operations
Manage System Log Configuration	Permits access to System Log Configuration (control the system log daemon, event logging, and the logs that are stored in the database)

8.7 Configuring Zones of Access for Multiple Service Providers

You can use security administration to allow two service providers to share access to equipment by setting up a separate zone of access for each service provider. For example, one service provider can be responsible for an iMAP chassis and some of its network or service cards, while another service provider is responsible for other network and service cards in the chassis. You can configure shared access to any equipment managed by the NMS.

Each service provider must have its own installation of the NMS. Before you begin, carefully plan out who will have access to the equipment and who will have their access restricted at each service provider. When you are ready to create the zones of access, do the following:

- Have all users log out of the NMS. All users must be logged off while you are making administrative changes to the user accounts.
- Back up the NMS. You must have a fresh backup available to restore the NMS and recover from errors during the configuration process.

Setting up zones of access requires two administrative operations:

- Setting permissions for groups, which determines what operations users in that group can perform, and,
- Creating custom view scopes for groups, which determines the objects on which users can perform the operations.

After you complete the configuration, back up the NMS again to save the configuration for future reference.

8.7.1 Example: Sharing Access Between Two Service Providers

This example demonstrates how two service providers can share access to an iMAP 9810 device. In this example, Provider #1 manages the chassis, CFCs, software upgrades, backups, network-facing interfaces, VLANs, EPSRs and other operations, as well as customer-facing interfaces on all cards except card 10. Provider #2 manages all customer-facing interfaces on card 10. The following figure illustrates this scenario:

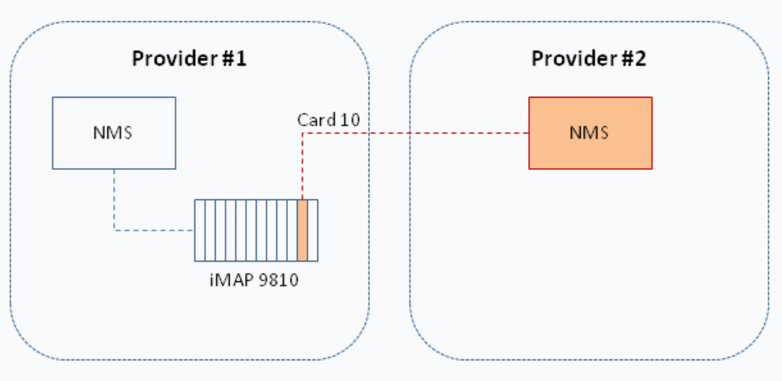


FIGURE 8-15 Zones of Access on iMAP 9810

The example uses two groups for each provider: **Admin** and **Users**. In both Provider #1 and Provider #2, the **Admin** group maintains the default settings to create users and groups. In Provider #1, the **Users** group is modified to prevent access to interfaces on card 10. In Provider #2, the **Users** group is modified to prevent access to chassis, network, and polling operations, and port management is restricted to card 10. Provider #2 **Users** group members can provision triple play customers, and view and modify alarms, events, ports, and iMGs, but they cannot perform switch-level operations beyond allowed interfaces, such as database backup, user administration, card management, statistics polling, SNMP configuration, or VLAN configuration.

Note: This example is just one scenario. You can add or remove permissions and provide access to different cards or equipment as needed.

The procedures to set up the scenario are:

- Set permissions for Provider #2
- Create custom view scopes for Provider #2
- Create custom view scopes for Provider #1

8.7.1.1 Setting Permissions for Provider #2

To set permissions for the **Users** group in Provider #2:

1. Log in to the NMS for Provider #2 with the root account.
2. Go to **Tools > Security Administration**. The Security Administration tool appears.

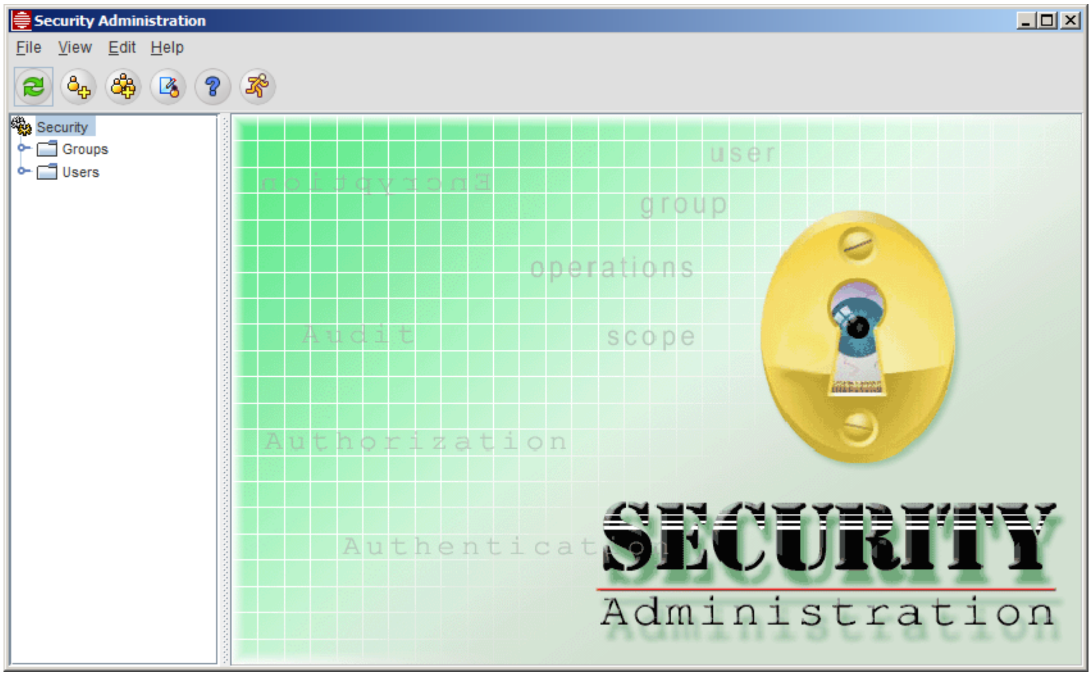
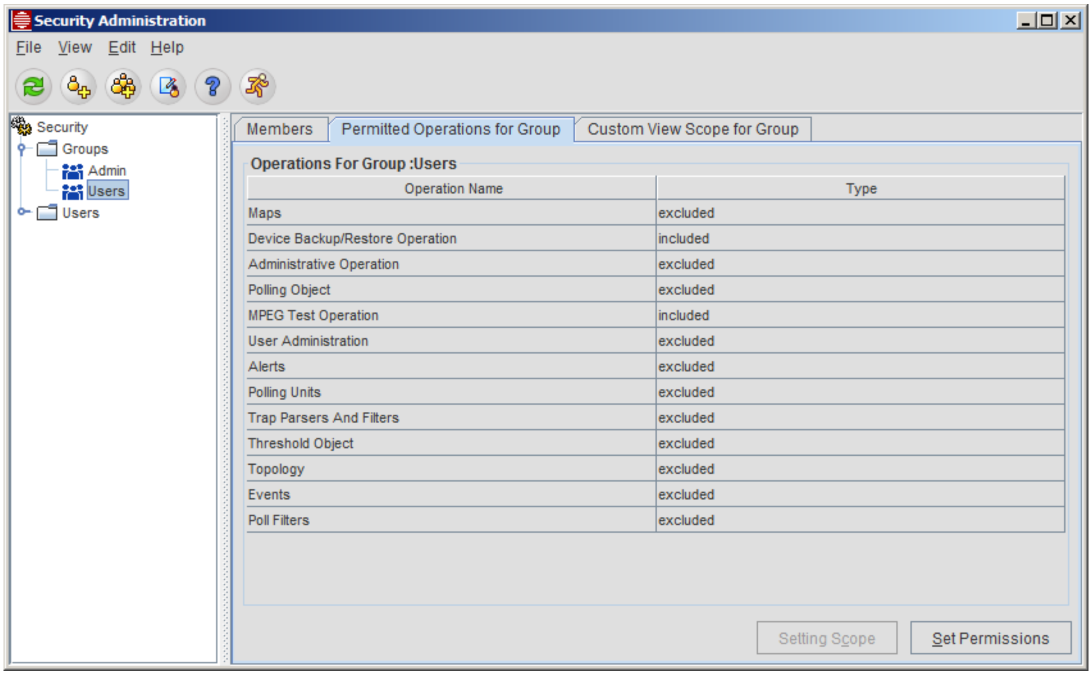


FIGURE 8-16 Security Administration

3. Expand the **Groups** folder, then select **Users**.

Note: Make sure you select Users group within the Groups folder, not the Users folder.

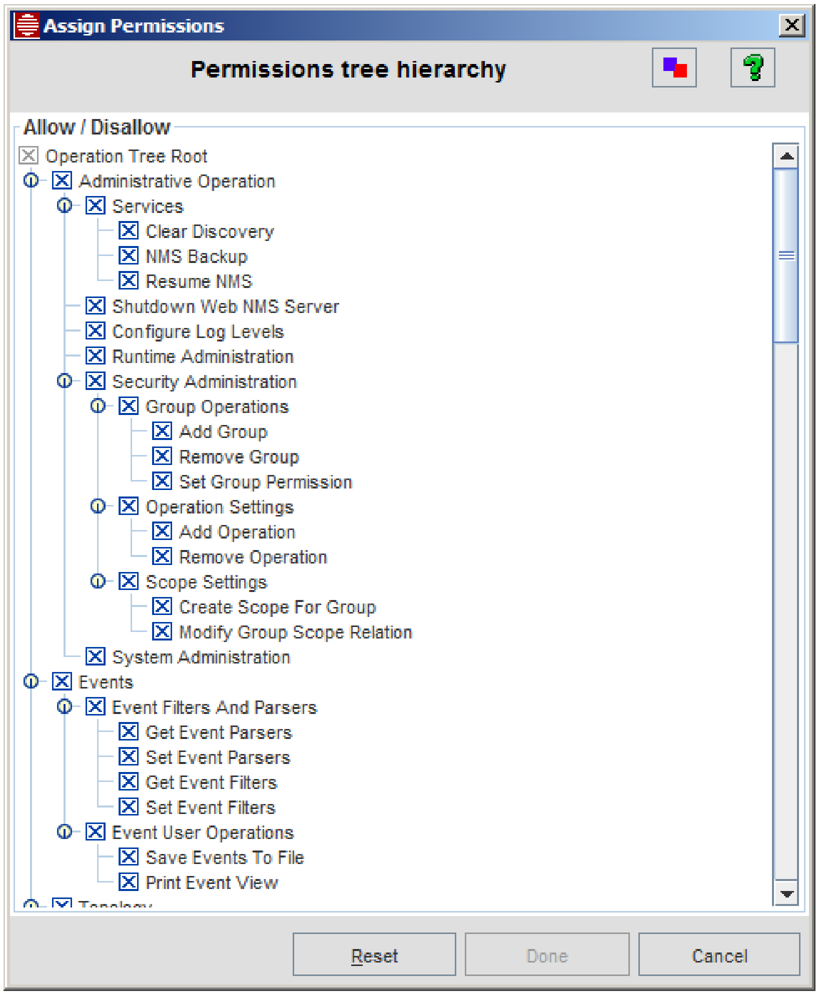


Operations For Group :Users

Operation Name	Type
Maps	excluded
Device Backup/Restore Operation	included
Administrative Operation	excluded
Polling Object	excluded
MPEG Test Operation	included
User Administration	excluded
Alerts	excluded
Polling Units	excluded
Trap Parsers And Filters	excluded
Threshold Object	excluded
Topology	excluded
Events	excluded
Poll Filters	excluded

FIGURE 8-17 Users Group

4. Select the **Permitted Operations for Group** tab, then click **Set Permissions**. The **Assign Permissions** box appears.



- ☒ Operation Tree Root
  - ☒ Administrative Operation
    - ☒ Services
      - ☒ Clear Discovery
      - ☒ NMS Backup
      - ☒ Resume NMS
    - ☒ Shutdown Web NMS Server
    - ☒ Configure Log Levels
    - ☒ Runtime Administration
    - ☒ Security Administration
      - ☒ Group Operations
        - ☒ Add Group
        - ☒ Remove Group
        - ☒ Set Group Permission
      - ☒ Operation Settings
        - ☒ Add Operation
        - ☒ Remove Operation
      - ☒ Scope Settings
        - ☒ Create Scope For Group
        - ☒ Modify Group Scope Relation
    - ☒ System Administration
  - ☒ Events
    - ☒ Event Filters And Parsers
      - ☒ Get Event Parsers
      - ☒ Set Event Parsers
      - ☒ Get Event Filters
      - ☒ Set Event Filters
    - ☒ Event User Operations
      - ☒ Save Events To File
      - ☒ Print Event View
  - ☒ Topology

FIGURE 8-18 Assign Permissions box

The **Assign Permissions** box contains 12 categories of operations:

- Administrative Operation
- Alerts
- AT Object Operation
- Events
- Maps
- Poll Filters
- Polling Object
- Polling Units
- Threshold Object
- Topology
- Trap Parsers And Filters
- User Administration

Note: *The categories of operations in the Permissions Tree Hierarchy are periodically reordered, and may appear in a different position in the tree each time you open the Assign Permissions box.*

Note: See "Permissions Tree Hierarchy" on page 170 for information on the operations available in the Permissions Tree Hierarchy.

5. To allow Provider #2 users to provision customers on the allowed interfaces, set the permissions as follows:

   Allow all of the operations in the following categories:

   - Alerts
   - Events

   Disallow all of the operations in the following categories:

   - Administrative Operation
   - Maps
   - Poll Filters
   - Polling Object
   - Polling Units
   - Threshold Object
   - Trap and Parsers
   - User Administration

   In the **Topology** category, allow and disallow the following:

   - Modify Object - Disallow
   - Add Network - Disallow
   - Add Note - Allow
   - Delete Object - Allow
   - Refresh Node - Allow

   In the **AT Object Operation** category, allow and disallow the operations according to Table 8-16. In some cases, some operations within a subcategory are allowed while others are disallowed.

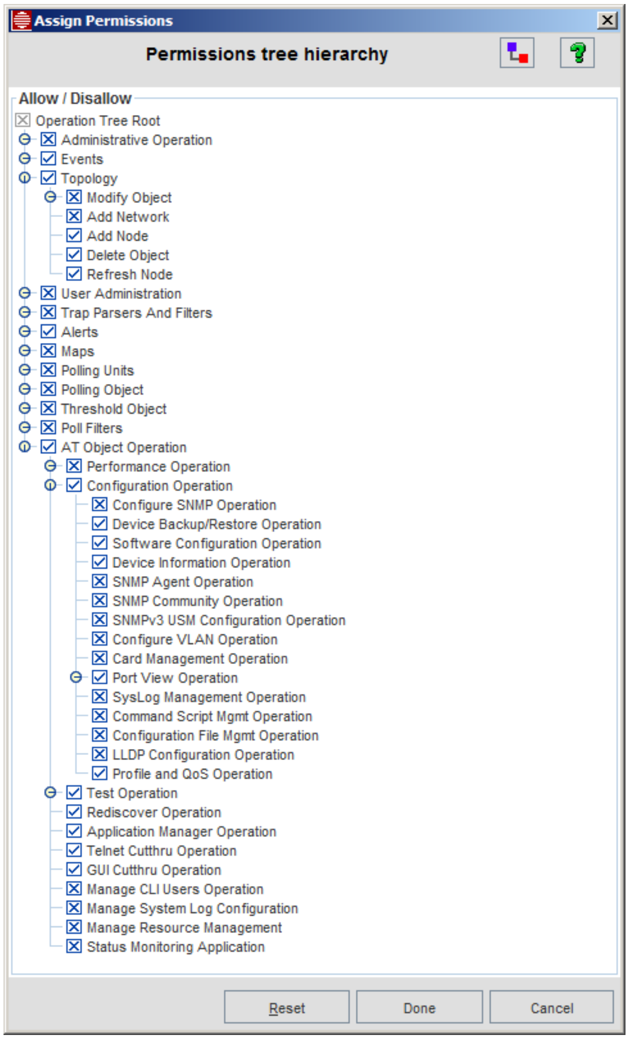
TABLE 8-16 **AT Object Operation Permissions for Provider #2**

Subcategory	Operation	Allow/Disallow
Application Manager Operation	-	Allow

TABLE 8-16 AT Object Operation Permissions for Provider #2 (Continued)

Subcategory	Operation	Allow/Disallow
Configuration Operation	Card Management Operation	Disallow
	Command Script Mgmt Operation	Disallow
	Configuration File Mgmt Operation	Disallow
	Configure SNMP Operation	Disallow
	Configure VLAN Operation	Disallow
	Device Backup/Restore Operation	Allow
	Device Information Operation	Allow
	LLDP Configuration Operation	Disallow
	Port View Operation	Allow
	Profile and QoS Operation	Allow
	SNMP Agent Operation	Disallow
	SNMP Community Operation	Disallow
	SNMPv3 USM Configuration Operation	Disallow
	Software Configuration Operation	Allow
	SysLog Management Operation	Disallow
GUI Cutthru Operation	-	Allow
Manage CLI Users Operation	-	Disallow
Manage Resource Management	-	Disallow
Manage System Log Configuration	-	Disallow
Performance Operation	Monitor Collections Operation	Disallow
	Statistics Operation	Disallow
Rediscover Operation	-	Allow
Status Monitoring Application	-	Disallow
Telnet Cutthru Operation	-	Allow
Test Operation	MPEG Test Operation	Allow

The final Permissions Tree Hierarchy should look similar to Figure 8-19.



Assign Permissions

Permissions tree hierarchy

Allow / Disallow

- ☒ Operation Tree Root
  - ☒ Administrative Operation
  - ☑ Events
  - ☑ Topology
    - ☒ Modify Object
    - ☒ Add Network
    - ☑ Add Node
    - ☑ Delete Object
    - ☑ Refresh Node
  - ☒ User Administration
  - ☒ Trap Parsers And Filters
  - ☑ Alerts
  - ☒ Maps
  - ☒ Polling Units
  - ☒ Polling Object
  - ☒ Threshold Object
  - ☒ Poll Filters
  - ☑ AT Object Operation
    - ☒ Performance Operation
    - ☑ Configuration Operation
      - ☒ Configure SNMP Operation
      - ☑ Device Backup/Restore Operation
      - ☑ Software Configuration Operation
      - ☑ Device Information Operation
      - ☒ SNMP Agent Operation
      - ☒ SNMP Community Operation
      - ☒ SNMPv3 USM Configuration Operation
      - ☒ Configure VLAN Operation
      - ☒ Card Management Operation
      - ☑ Port View Operation
      - ☒ SysLog Management Operation
      - ☒ Command Script Mgmt Operation
      - ☒ Configuration File Mgmt Operation
      - ☒ LLDP Configuration Operation
      - ☑ Profile and QoS Operation
    - ☑ Test Operation
    - ☑ Rediscover Operation
    - ☑ Application Manager Operation
    - ☑ Telnet Cutthru Operation
    - ☑ GUI Cutthru Operation
    - ☒ Manage CLI Users Operation
    - ☒ Manage System Log Configuration
    - ☒ Manage Resource Management
    - ☒ Status Monitoring Application

FIGURE 8-19 Provider #2 Permissions

If necessary, you can disallow some of the operations listed as allowed, such as **Alerts**, **Events**, or **Device Backup/Restore Operation**, depending on your local procedures and users' responsibilities. **Port View** and **Port Provision** operations must be enabled to provision triple play customers.

8.7.1.2 Creating Custom View Scopes for Provider #2

To set custom view scopes for the **Users** group in Provider #2:

1. Log in to the NMS for Provider #2 with the root account.
2. Go to **Tools > Security Administration**. The Security Administration tool appears.

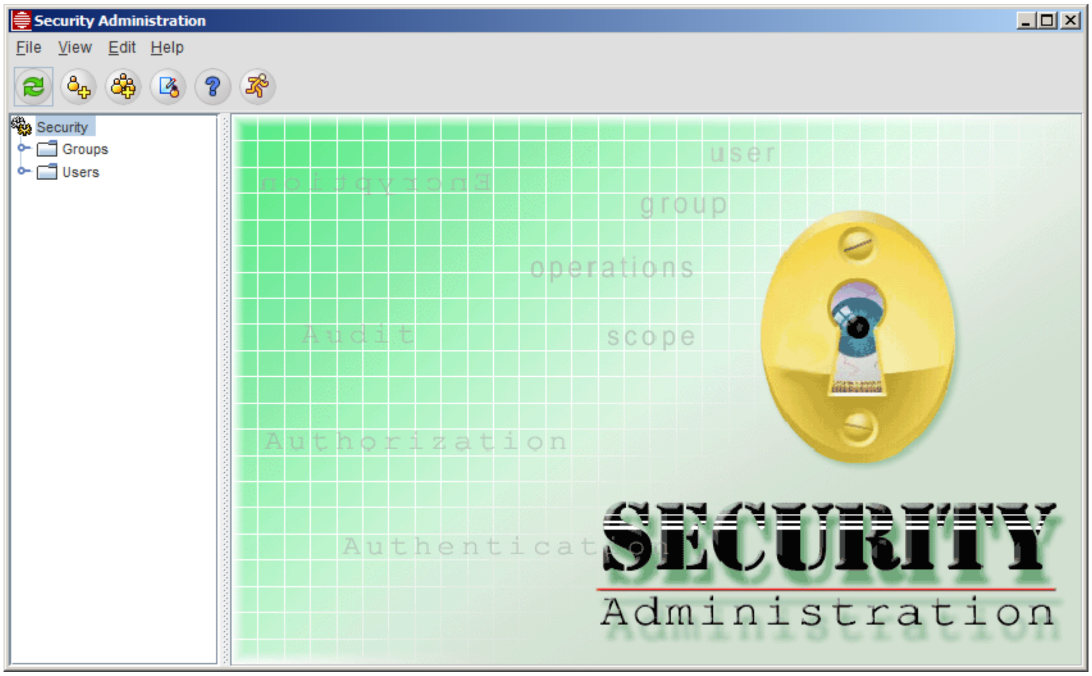
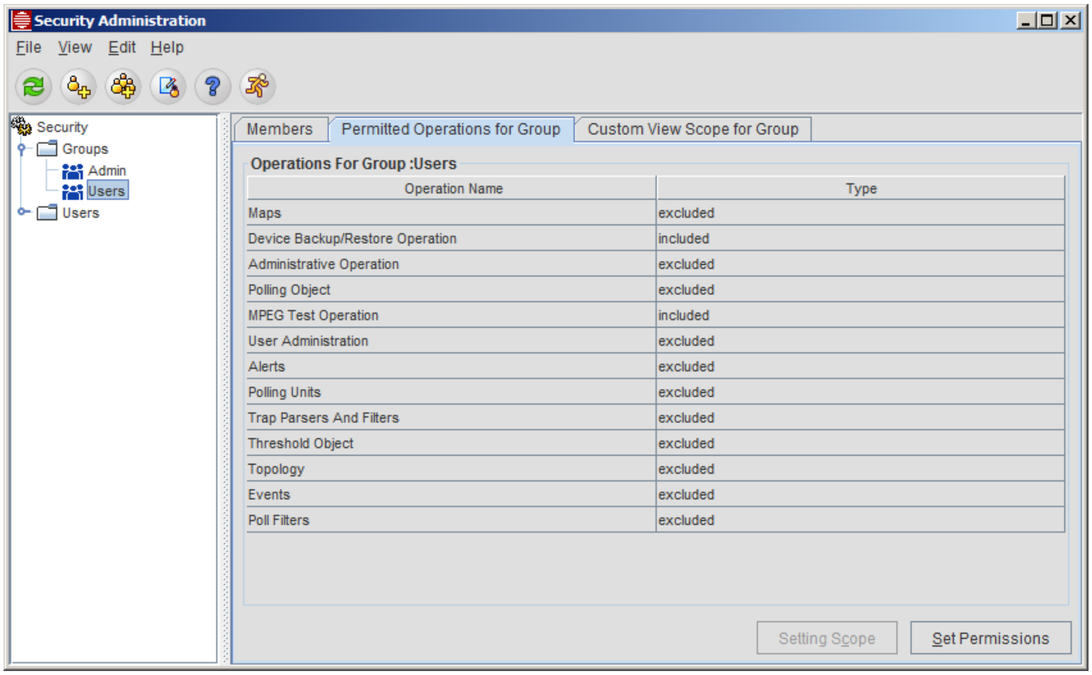


FIGURE 8-20 Security Administration

3. Expand the **Groups** folder, then select **Users**.

Note: Make sure you select Users group within the Groups folder, not the Users folder.



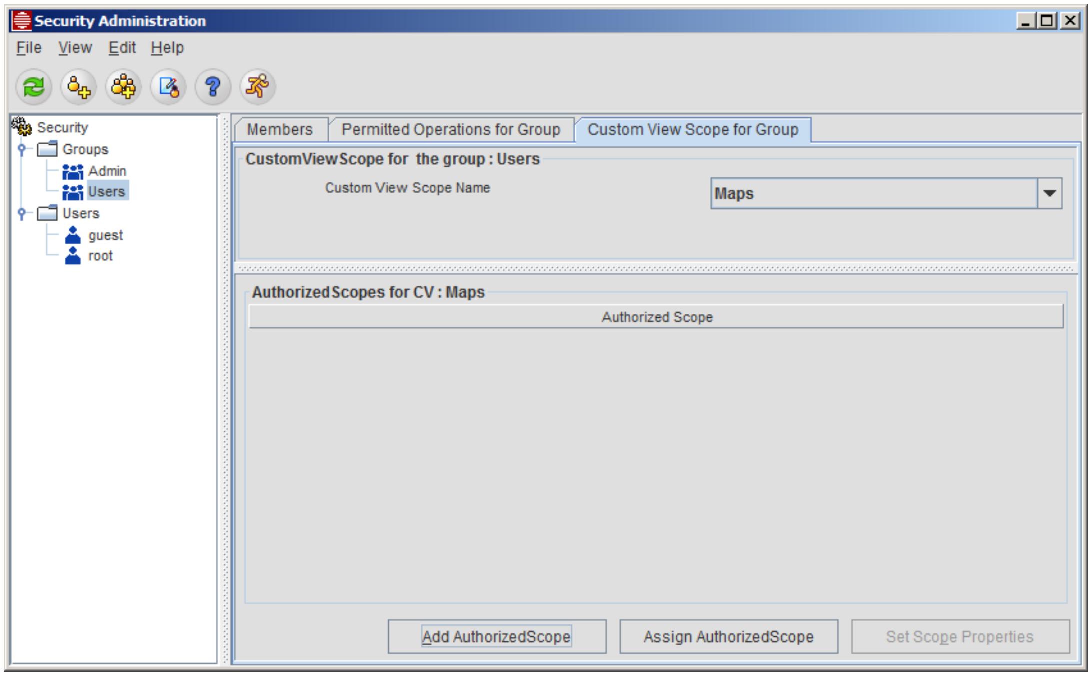
Operations For Group :Users

Operation Name	Type
Maps	excluded
Device Backup/Restore Operation	included
Administrative Operation	excluded
Polling Object	excluded
MPEG Test Operation	included
User Administration	excluded
Alerts	excluded
Polling Units	excluded
Trap Parsers And Filters	excluded
Threshold Object	excluded
Topology	excluded
Events	excluded
Poll Filters	excluded

FIGURE 8-21 Users Group

4. Select the **Custom View Scope for Group** tab.

5. In the **Custom View Scope Name** drop-down list, select the view scope you want to create (for example: **Maps**). Table 8-17 lists the custom view scope settings for this example.



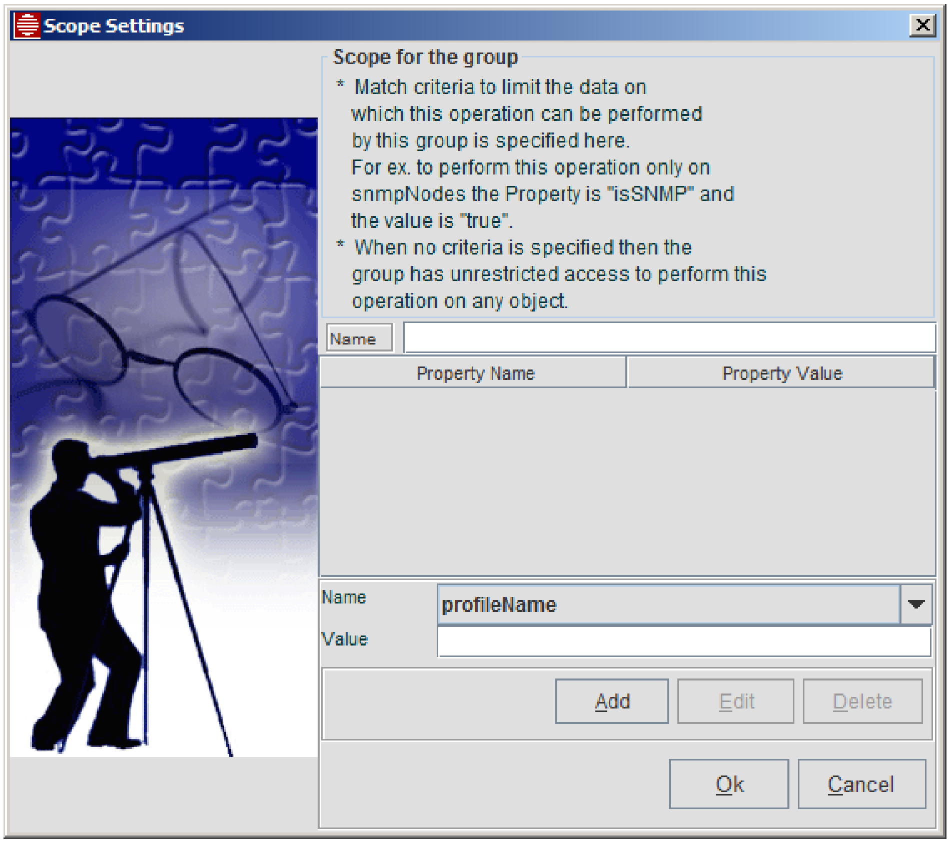
CustomViewScope for the group : Users

Custom View Scope Name: Maps

AuthorizedScopes for CV : Maps

FIGURE 8-22 Custom View Scope for Groups - Maps

6. Click **Add AuthorizedScope**. The **Scope Settings** box appears.



Scope for the group

* Match criteria to limit the data on which this operation can be performed by this group is specified here. For ex. to perform this operation only on snmpNodes the Property is "isSNMP" and the value is "true".

* When no criteria is specified then the group has unrestricted access to perform this operation on any object.

Name

Name: profileName

Value

FIGURE 8-23 Scope Settings

7. Create the following custom view scopes:

TABLE 8-17 Custom View Scopes for Provider #2

Custom View Scope for Group tab	Scope Settings box		
Custom View Scope Name	Name (upper field)	Name (lower field drop-down list)	Value
Maps	Map-Scope	upstreamDevicePort	10.52.30.39_10.*
Network Database	Type-Scope	type	profile
Network Database	Port-Scope	name	10.52.30.39_10.*
Network Database	iMG-Scope	upstreamDevicePort	10.52.30.39_10.*

The **Value** field contains the match criteria. In this example, Provider #2 users have access to all interfaces on device 10.52.30.39, card 10. Since this is an iMAP device and is discovered by its IP address, the match syntax for all interfaces on card 10 is **10.52.30.39_10.***.

Note: The NMS normally assigns the upstream device port to the iMG's sysLocation field. You can use sysLocation instead of upstreamDevicePort as the property name for the iMG-Scope in the example, however, the sysLocation field is blank for iMGs provisioned from TFTP boot configurations or MAC addresses. In these cases, alternative match criteria are required.

Note: See "Setting Scope Properties" on page 168 for information on specifying match criteria for custom view scopes.

8. Click **Add** to add the match criteria for the view scope, then click **Ok** to save the view scope.

The custom view scopes affect the following screens for the **Users** group:

TABLE 8-18 Custom View Scope Results for Provider #2

Custom View Scope Name	Network Objects Screen	Result
Map-Scope	Network Maps > IP Network	Displays provisioned iMGs connected to interfaces on card 10.
Type-Scope	Network Service Data > Profiles	Displays all profiles.
Port-Scope	Network Inventory > Ports	Displays all interfaces on card 10.
iMG-Scope	Network Inventory > iMG/RGs	Displays provisioned iMGs connected to interfaces on card 10.

8.7.1.3 Creating Custom View Scopes for Provider #1

To set custom view scopes for the **Users** group in Provider #1:

1. Log in to the NMS for Provider #1 with the root account.
2. Go to **Tools > Security Administration**. The Security Administration tool appears.

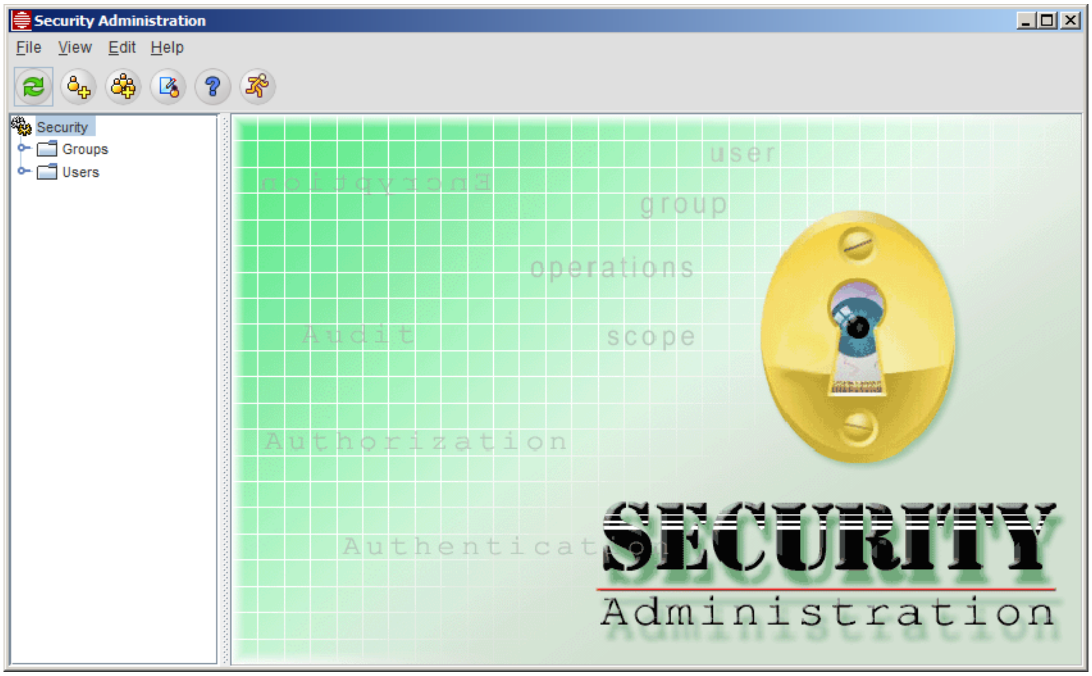
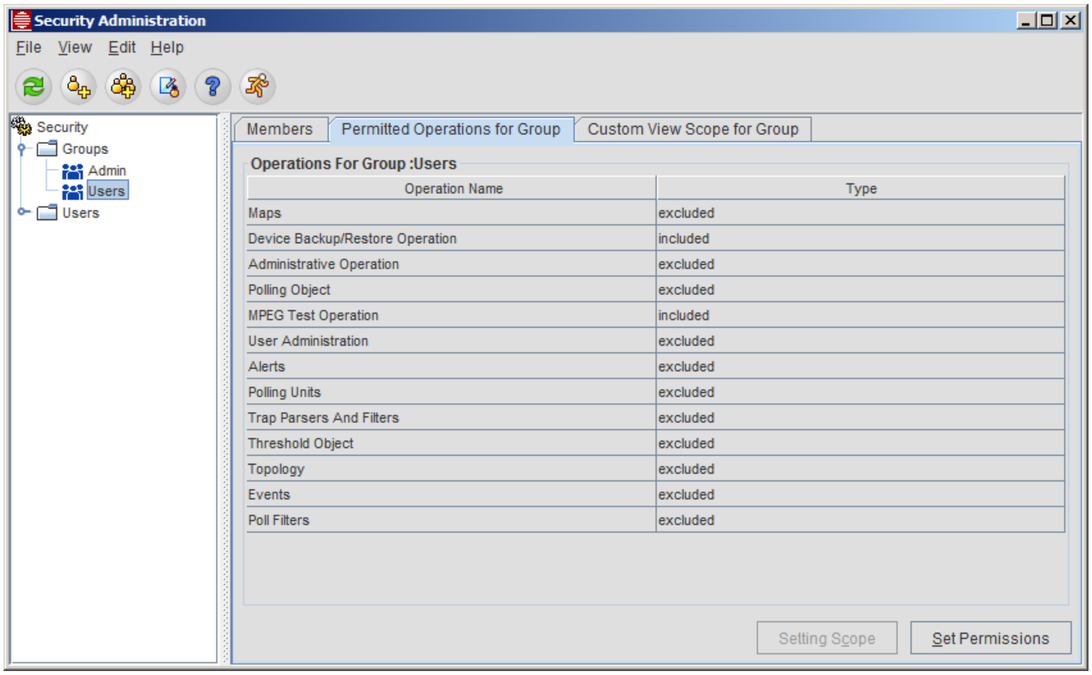


FIGURE 8-24 Security Administration

3. Expand the **Groups** folder, then select **Users**.

Note: Make sure you select Users group within the Groups folder, not the Users folder.



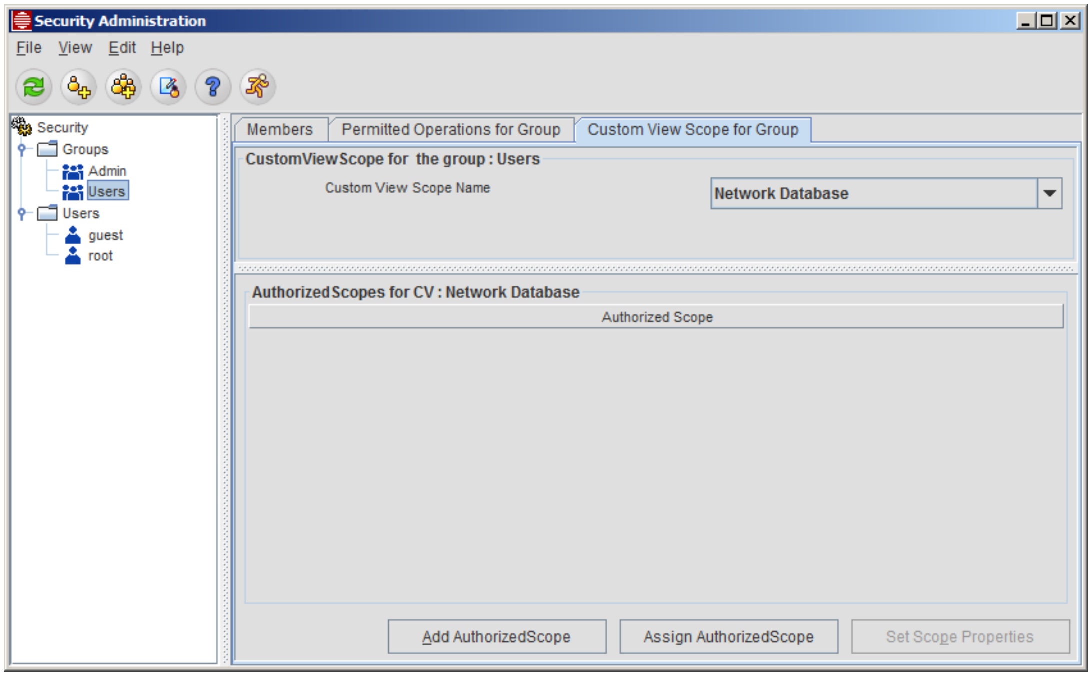
Operations For Group :Users

Operation Name	Type
Maps	excluded
Device Backup/Restore Operation	included
Administrative Operation	excluded
Polling Object	excluded
MPEG Test Operation	included
User Administration	excluded
Alerts	excluded
Polling Units	excluded
Trap Parsers And Filters	excluded
Threshold Object	excluded
Topology	excluded
Events	excluded
Poll Filters	excluded

FIGURE 8-25 Users Group

4. Select the **Custom View Scope for Group** tab.

5. In the **Custom View Scope Name** drop-down list, select the view scope you want to create (for example: **Network Database**). Table 8-19 lists the custom view scope settings for this example.



CustomViewScope for the group : Users

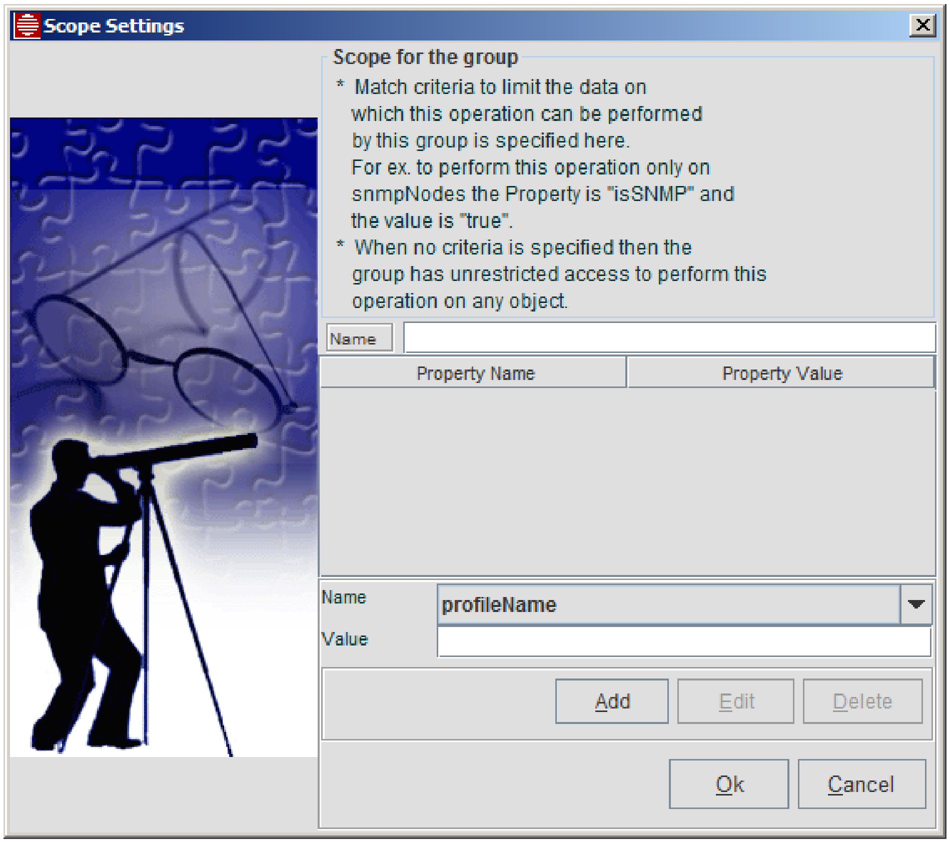
Custom View Scope Name: Network Database

AuthorizedScopes for CV : Network Database

Authorized Scope

FIGURE 8-26 Custom View Scope for Groups - Network Database

6. Click **Add AuthorizedScope**. The **Scope Settings** box appears.



Scope for the group

* Match criteria to limit the data on which this operation can be performed by this group is specified here. For ex. to perform this operation only on snmpNodes the Property is "isSNMP" and the value is "true".

* When no criteria is specified then the group has unrestricted access to perform this operation on any object.

Name

Property Name	Property Value

Name: profileName

Value

FIGURE 8-27 Scope Settings

7. Create the following custom view scopes:

TABLE 8-19 Custom View Scopes for Provider #1

Custom View Scope for Group tab	Scope Settings box		
Custom View Scope Name	Name (upper field)	Name (lower field drop-down list)	Value
Network Database	Type-Scope	type	profile
Network Database	Port-Scope	name	!10.52.30.39_10.*
Network Database	iMG-Scope	upstreamDevicePort	!10.52.30.39_10.*

The **Value** field contains the match criteria. In this example, Provider #1 users should not have access to all interfaces on device 10.52.30.39, card 10. Since this is an iMAP device and is discovered by its IP address, the match syntax to exclude all interfaces on card 10 is **!10.52.30.39_10.***.

8. Click **Add** to add the match criteria for the view scope, then click **Ok** to save the view scope.

The custom view scopes affect the following screens for the **Users** group:

TABLE 8-20 Custom View Scope Results for Provider #1

Custom View Scope Name	Network Objects Screen	Result
Type-Scope	Network Service Data > Profiles	Displays all profiles.
Port-Scope	Network Inventory > Ports	Hides all interfaces on card 10.
iMG-Scope	Network Inventory > iMG/RGs	Hides provisioned iMGs connected to interfaces on card 10.

8.7.2 Extending the Two Service Provider Example

The example in "Example: Sharing Access Between Two Service Providers" on page 176 illustrates a simple scenario between two service providers. In reality, zones of access between service providers will probably be more complex. Based on your site requirements, you can modify Provider #1 and Provider #2's permissions in a myriad of ways, such as:

- Restricting access to fault management
- Providing access to card or performance management
- Providing (or restricting) access to interfaces on additional cards

8.7.2.1 Adding Additional Cards and Interfaces

In the example, Provider #2 has access to all interfaces on card 10, designated as **10.52.30.39_10.***. You can extend access to the interfaces on cards 8 and 9 with the match criteria syntax:

10.52.30.39_8.*, 10.52.30.39_9.*, 10.52.30.39_10.*

Since the match criteria value has a limit of 50 characters, you may need to break up a single view scope into multiple view scopes, such as one view scope per card. To extend the example to include interfaces on cards 8 and 9 with multiple view scopes, you would create the custom view scopes in Table 8-21 instead of those listed in Table 8-17:

TABLE 8-21 Extended Custom View Scopes for Provider #2

Custom View Scope for Group tab	Scope Settings box		
Custom View Scope Name	Name (upper field)	Name (lower field drop-down list)	Value
Maps	Map-08	upstreamDevicePort	10.52.30.39_8.*
Maps	Map-09	upstreamDevicePort	10.52.30.39_9.*
Maps	Map-10	upstreamDevicePort	10.52.30.39_10.*
Network Database	Type-Scope	type	profile
Network Database	Port-08	name	10.52.30.39_8.*
Network Database	Port-09	name	10.52.30.39_9.*
Network Database	Port-10	name	10.52.30.39_10.*
Network Database	iMG-08	upstreamDevicePort	10.52.30.39_8.*
Network Database	iMG-09	upstreamDevicePort	10.52.30.39_9.*
Network Database	iMG-10	upstreamDevicePort	10.52.30.39_10.*

If Provider #2 users require card management in addition to interface management, the Network Database view scopes need to include match criteria for cards in addition to interfaces. In the example, the match criteria syntax for card 10 and its interfaces is:

10.52.30.39_10,10.52.30.39_10.*

The wildcard character (*) means “match all characters following.” The syntax **10.52.30.39_10*** (without the period after “10”) would include card 10 and all of its interfaces. The syntax **10.42.30.39_1***, however, would include all of the interfaces on card 1, as well as cards 11-19 and all of their interfaces.

If you are sharing cards across multiple chassis, reorganizing the cards can simplify the operation. See "Customer Cutover" on page 352 for information on moving iMGs from one card to another while minimizing downtime.

8.7.2.2 Selecting Devices on a Subnet

You can select iMGs by IP address and use the wildcard operator to select all devices on a subnet. If all of Provider #2’s iMGs are in the subnet 10.52.31.0/24, you can create the following custom view scope to capture them:

TABLE 8-22 Custom View Scope for Provider #2 iMGs on a Subnet

Custom View Scope for Group tab	Scope Settings box		
Custom View Scope Name	Name (upper field)	Name (lower field drop-down list)	Value
Network Database	iMG-31	ipAddress	10.52.31*

The custom view scope in Table 8-22 selects all of the devices that are discovered on the subnet, not just provisioned iMGs.

8.8 Remote Authorization (RADIUS / Tacacs+) on Devices

RADIUS and Tacacs+ are remote authentication protocols used by devices to authenticate telnet user-client sessions. When the user logs in, the device forwards all login information to the RADIUS servers first, followed by the Tacacs+ servers (if RADIUS is not available) for authentication until it receives a response back from one of them. Depending on the exchange of messages, the device grants or denies access for the session. RADIUS uses UDP/IP for transmitting information across the network, while Tacacs+ uses TCP/IP.

Note: *For complete information on the RADIUS / Tacacs+ protocol and how they are handled by Allied Telesis devices, refer to the iMAP Software Reference Manual and AlliedWare Plus Reference Manuals.*

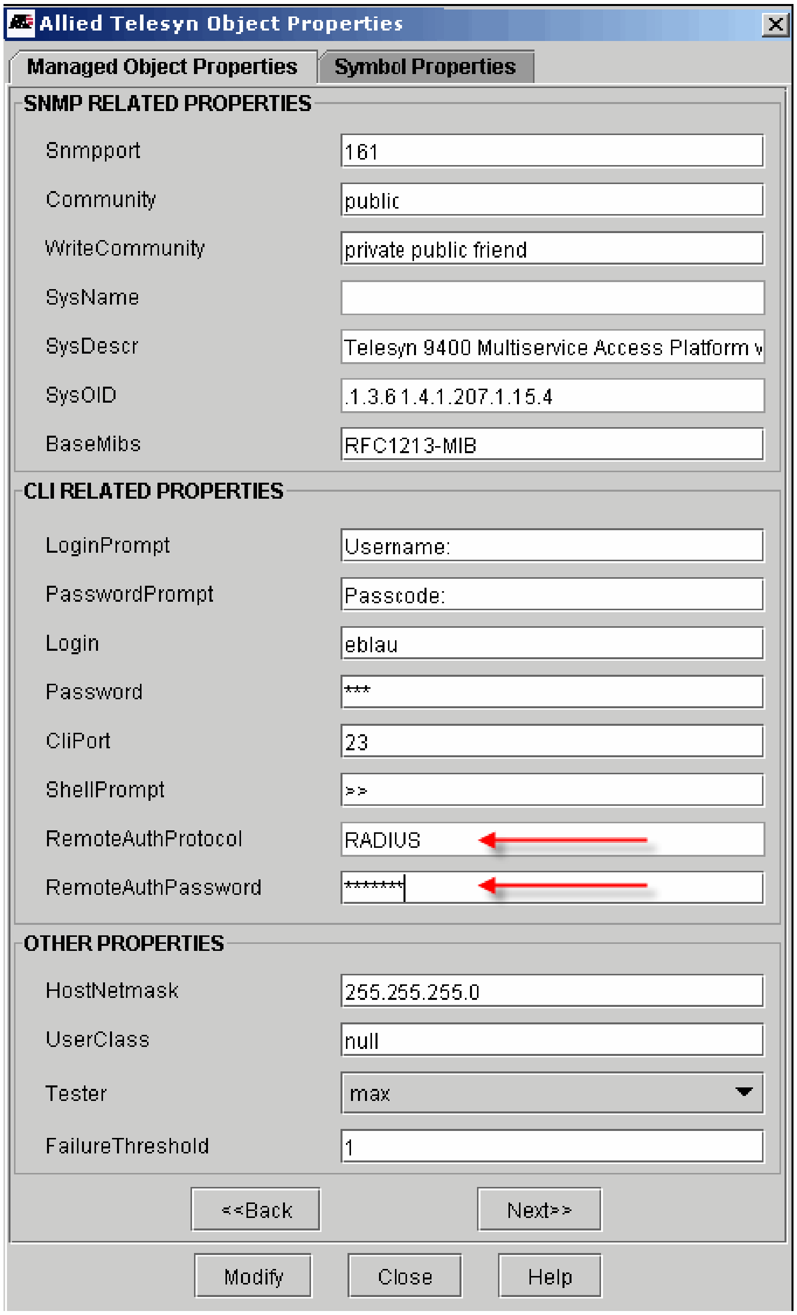
When the AlliedView NMS is initially configured and logs in to a device that is configured with RADIUS/Tacacs+, only a user-level privilege can be assigned. To allow for security officer level, the client must send a special "ENABLE SECURITY OFFICER" command string ("ENABLE" for AlliedWare Plus devices) back to the server. The server prompts for a "Passcode" ("Password for AlliedWare Plus devices). The client then transmits the appropriate passcode (password) after which the session has a Security Officer level (level 15).

Note: *Only iMAP (15.1 and up) and AlliedWare Plus (5.4.2 and up) devices support Tacacs+.*

Note: *Devices other than iMAPs supporting RADIUS provide a direct "SECURITY" access after first authentication, if discovered as the "SECURITY" level user.*

8.8.1 RADIUS

For devices that use the RADIUS, authentication is done on a per device basis that is datafilled for the device's MO properties. Refer to the following figure.



SNMP RELATED PROPERTIES

Snmpport	161
Community	public
WriteCommunity	private public friend
SysName	
SysDescr	Telesyn 9400 Multiservice Access Platform v
SysOID	.1.3.6.1.4.1.207.1.15.4
BaseMibs	RFC1213-MIB

CLI RELATED PROPERTIES

LoginPrompt	Username:
PasswordPrompt	Passcode:
Login	eblau
Password	***
CliPort	23
ShellPrompt	>>
RemoteAuthProtocol	RADIUS
RemoteAuthPassword	*******

OTHER PROPERTIES

HostNetmask	255.255.255.0
UserClass	null
Tester	max
FailureThreshold	1

FIGURE 8-28 Filling out the MO Property Form for Remote Authentication

8.8.2 Tacacs+

For Tacacs+, the user can provision on a per-device basis as well, but the administrator can also provision this on a system-wide basis, using the special User ID TACPLUS_USER, and then filling in the appropriate password.

When the user selects *Tools -> Manage CLI Users*, the Discovery Configurator with the CLI Logins tab appears.

8.9 NMS RADIUS Client Support

The NMS supports RADIUS authentication for NMS user logins. An open source RADIUS client is integrated into the NMS server, using a central RADIUS server on the customer's network.

Note: *RADIUS is specified in RFC 2865 (http://www.ietf.org/rfc/rfc2865.txt).*

The NMS Security Management feature, as explained in "Adding a New Group" on page 163, has pre-defined groups (Users and Admin) with default permissions. Moreover, custom groups can be added. The Security Management and NMS RADIUS Client Support feature need to be coordinated to ensure that these groups and permissions are usable to the RADIUS-authenticated users. This is explained in detail in the rest of this section, especially "Feature Interactions (RADIUS Server De-activated or Unavailable)" on page 203.

Activation of this feature involves provisioning in two main areas:

9. At the RADIUS server, accounts are defined in the RADIUS database according to the configuration procedures of the RADIUS platform selected (Free RADIUS, Cisco Secure ACS etc.). Accounts are given passwords and assigned to permission groups.
10. At the NMS server, RADIUS authentication is enabled or disabled from an Authorization Configurator GUI, as explained in "RADIUS Configurator Tool (with Valid License)" on page 193.

Note: *Provisioning at the RADIUS server is outside the control of this feature, but is required and must be provisioned correctly for this feature to function correctly. Moreover, there are many RADIUS server distributions, and all should be compatible, but the example inputs are for FreeRADIUS and Cisco Secure ACS.*

The following figures provide an overview of the process and steps to activate RADIUS (the steps to deactivate are essentially the reverse).

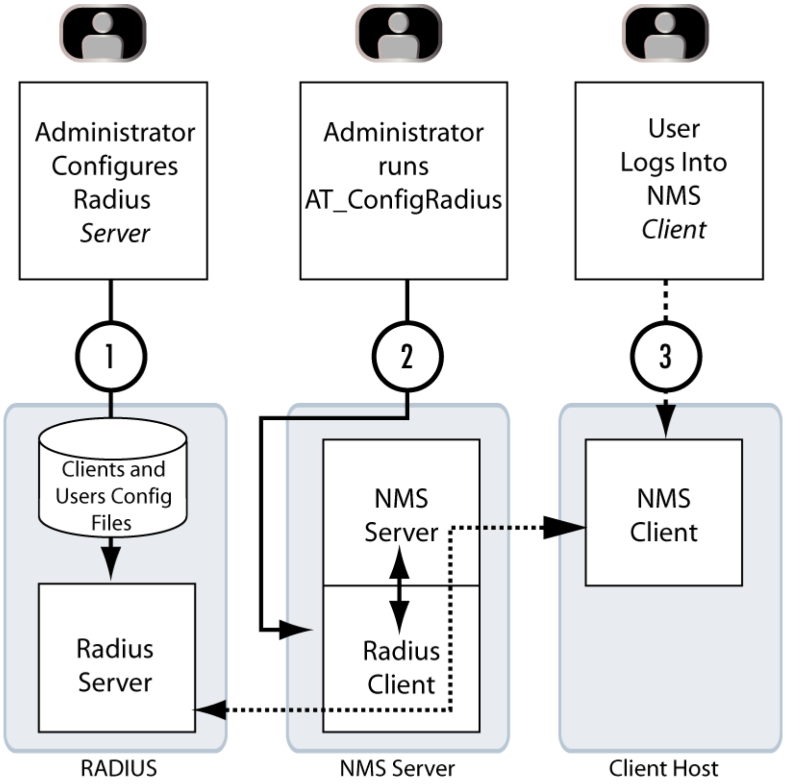

Administrator Configures Radius *Server*
Administrator runs AT_ConfigRadius
User Logs Into NMS *Client*
1
2
3
Clients and Users Config Files
Radius Server
NMS Server
Radius Client
NMS Client
RADIUS
NMS Server
Client Host

FIGURE 9 The NMS Server with RADIUS Client

8.9.1 RADIUS Configurator Tool (with Valid License)

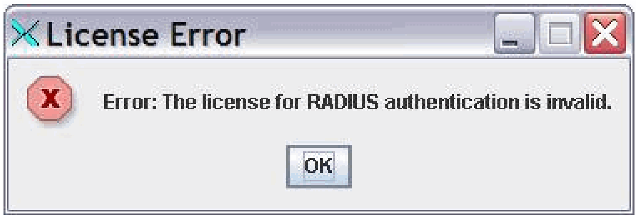
Once this feature is installed the login procedure is transparent; the client interface is the same with or without RADIUS authentication.

The main change to the NMS server is the addition of the AT_ConfigureRadius tool. To launch the tool:

1. On Windows, double-click **AT_ConfigureRadius.bat** in the <NMS_HOME>\bin directory.
2. On Linux, execute **AT_ConfigureRadius.sh** in the <NMS_HOME>/bin directory.
3. In a non-windows Linux environment, running the tool with the command ./AT_ConfigureRadius.sh

Methods 1 and 2 bring up the RADIUS Configurator GUI; method 3 uses a command interface. Each interface is explained below.

Note: This tool is only available if the user has a license with the RADIUS feature registered. If not, the following message appears when double-clicking on the **AT_ConfigureRadius.bat** *icon.*



License Error

Error: The license for RADIUS authentication is invalid.

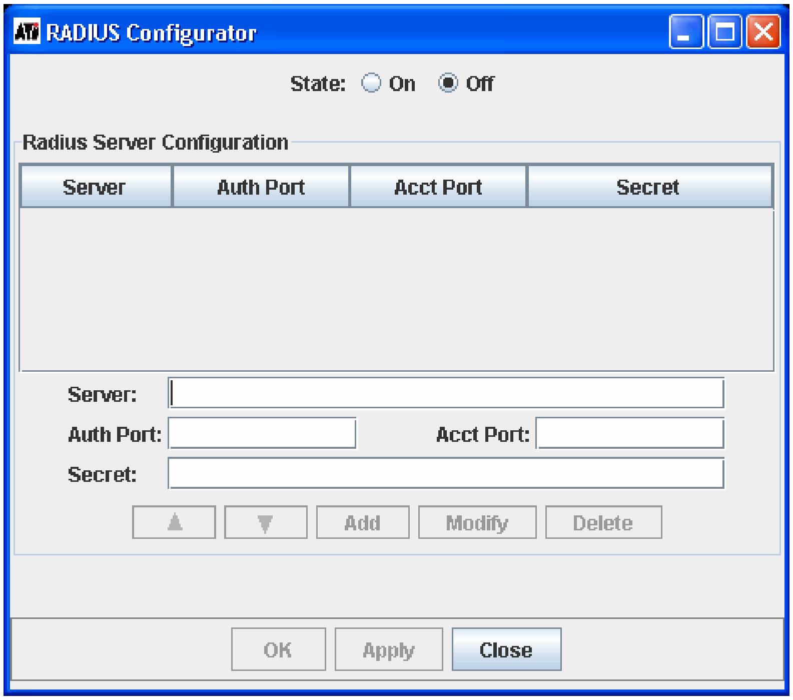
FIGURE 8-1 Error Message for Invalid License

The purpose of this tool is to configure the NMS *server* as a RADIUS *client*-that is, enable/disable RADIUS authentication and create a list of server contact information (address and port) and shared secrets to be used during authentication when enabled.

The shared secret is an encryption key stored separately on both platforms (RADIUS server and RADIUS client) and is never transmitted over the network.

8.9.1.1 GUI Interface

The first time the tool is launched, it shows the state is “Off” and shows no parameters, as shown in the following figure:



State: ○ On ● Off

Radius Server Configuration

Server	Auth Port	Acct Port	Secret

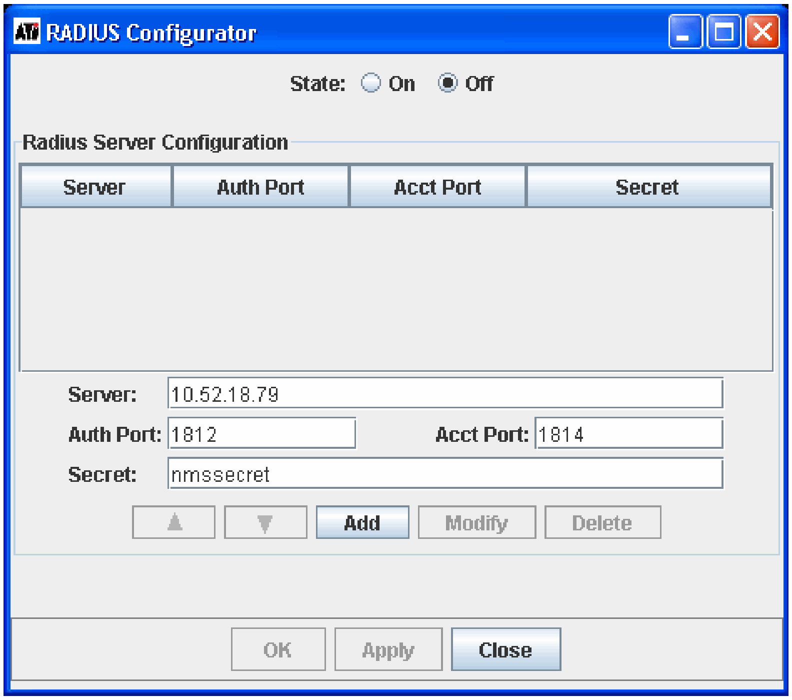
Server:

Auth Port: Acct Port:

Secret:

FIGURE 9 RADIUS Configurator - Initial Screen

Servers can be added via the fields on the lower part of the display. Notice the “Add” button becomes enabled when all the necessary parameters have been entered:



State: ○ On ● Off

Server	Auth Port	Acct Port	Secret

Server: 10.52.18.79

Auth Port: 1812 Acct Port: 1814

Secret: nmssecret

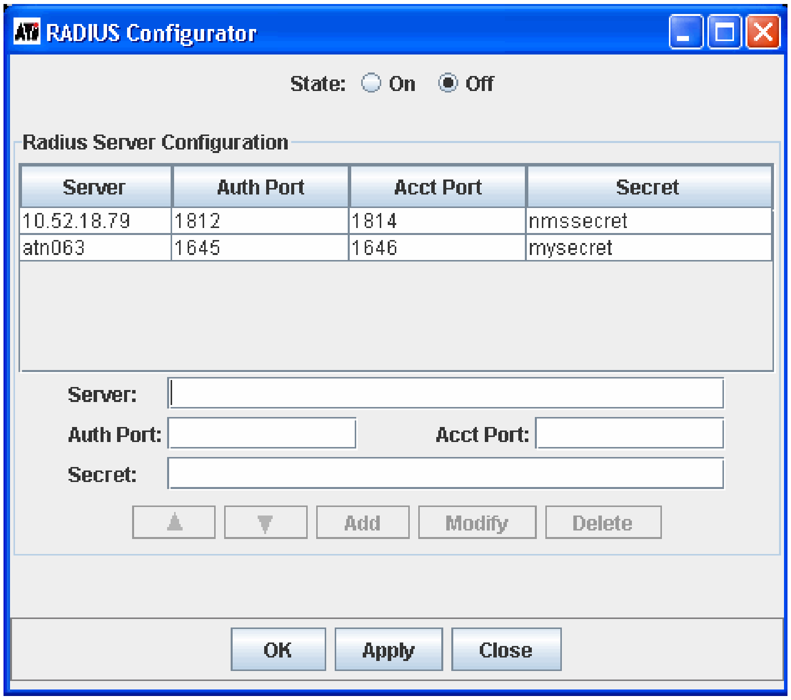
FIGURE 10 RADIUS Configurator - Initial Screen - Adding a Server

Multiple servers can be added. Servers can be designated by IP addresses or valid host names. During login, the authentication process will try each server in the order displayed, from top to bottom, until one server accepts the authentication request or all servers have rejected it. The order can be changed with the arrow buttons. Note that:

- The Add button will not allow adding a server that already exists in the table.
- The Modify button will allow any change to any field as long as it won't change the server to one that already exists in the table.

Note: *This tool cannot tell when host names map to existing IP addresses or not. Therefore the Add button will allow adding duplicate servers when they have different host names.*

Note: *There is no limit to the number of servers allowed, but more than 2 or 3 unreachable servers will cause long delays to users trying to log in because each server is tried one at a time and must timeout before the next server is tried. Therefore, servers with a history of unavailability should not be used for RADIUS authentication.*

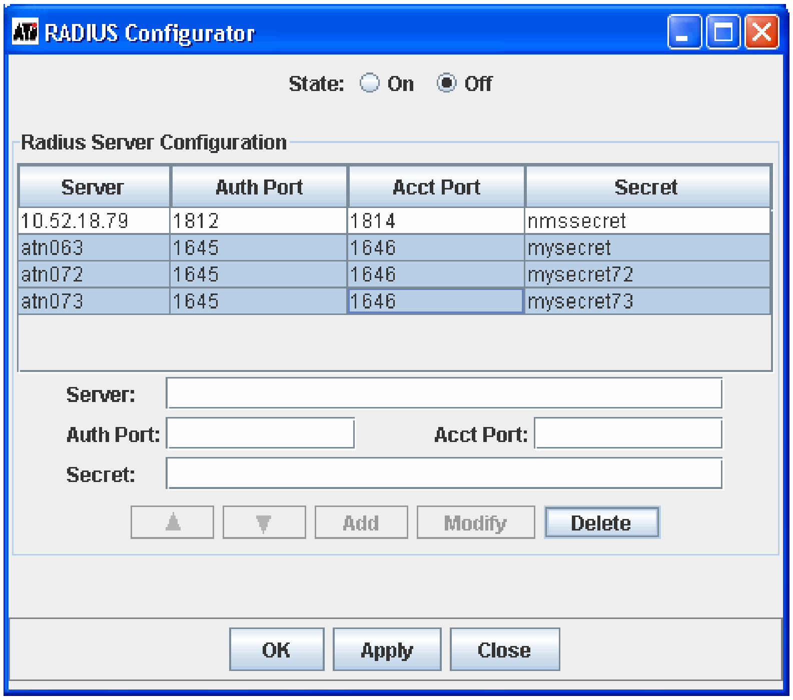


State: ○ On ● Off

Server	Auth Port	Acct Port	Secret
10.52.18.79	1812	1814	nmssecret
atn063	1645	1646	mysecret

FIGURE 11 RADIUS Configurator - Servers Added

Whereas only one server may be added at a time and only one may be modified at a time, multiple servers may be deleted by selecting multiple rows and clicking on the Delete button.



State: ○ On ● Off

Server	Auth Port	Acct Port	Secret
10.52.18.79	1812	1814	nmssecret
atn063	1645	1646	mysecret
atn072	1645	1646	mysecret72
atn073	1645	1646	mysecret73

Server:

Auth Port: Acct Port:

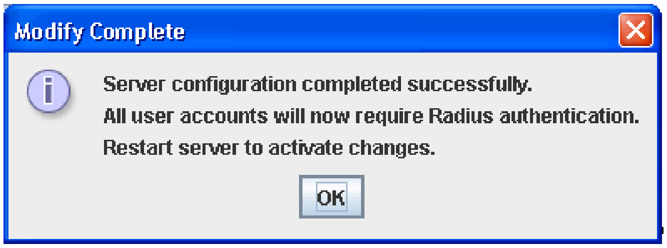
Secret:

FIGURE 12 RADIUS Configurator - Deleting Servers

Changes are not saved until you click **OK** or **Apply**.

Note: When activating the NMS client, set the Status to 'On' before selecting **OK** *or* **Apply**.

All changes won't take effect until the server is restarted. So after changing the State to 'On" and selecting OK or Apply, the modifications are completed and the tool displays the following message:


Modify Complete

Server configuration completed successfully.
All user accounts will now require Radius authentication.
Restart server to activate changes.

FIGURE 13 Message - RADIUS Configured, need to Restart

Note: When RADIUS is activated or deactivated, the NMS server is shut down. It must then be restarted.

Once RADIUS authentication is enabled, the only users that can log in are the ones previously defined in the RADIUS server(s).

8.9.1.2 Command Line Mode

The AT_ConfigureRadius tool can also be used in a command line mode, which is useful in a non-window Linux environment. Command line mode is invoked by running the tool from the command with one or more arguments, as demonstrated by the help command:

```
./AT_ConfigureRadius.sh help
    help
    print
    add [pos] server authport acctport secret
    remove server
    enable
    disable
```

- Print displays the current configuration.
- Add adds a new server with the specified authport, accounting port, and secret. The optional pos argument allows specifying a position in the list of servers.
- Remove removes the specified server.
- Enable enables RADIUS authentication and disable disables it.

The following is an example session:

```
$ ./AT_ConfigureRadius.sh add 10.52.18.78 1645 1646 nmssecret

 RADIUS Authentication State=DISABLED

 Server       Auth Port   Acct Port   Secret
 -----------  ---------   ---------   ---------
 10.52.18.79    1812        1814       nmssecret
 10.52.18.78    1645        1646       nmssecret

$ ./AT_ConfigureRadius.sh add 2 10.52.18.77 1812 1814 nmssecret

   RADIUS Authentication State=DISABLED

   Server       Auth Port   Acct Port   Secret
   -----------  ---------   ---------   ---------
   10.52.18.79    1812        1814        nmssecret
   10.52.18.77    1812        1814        nmssecret
   10.52.18.78    1645        1646        nmssecret

$ ./AT_ConfigureRadius.sh enable

   RADIUS Authentication State=ENABLED

   Server         Auth Port    Acct Port    Secret
   -----------    ---------    ---------    ---------
   10.52.18.79    1812        1814        nmssecret
   10.52.18.77    1812        1814        nmssecret
   10.52.18.78    1645        1646        nmssecret

// Restart NMS server to activate changes.
$ ./AT_ConfigureRadius.sh remove 10.52.18.77

   RADIUS Authentication State=ENABLED

   Server         Auth Port    Acct Port    Secret
   -----------    ---------    ---------    ---------
   10.52.18.79    1812        1814        nmssecret
   10.52.18.78    1645        1646        nmssecret
```

8.9.2 Example Configurations

The following examples go through setting up of the NMS RADIUS Client Support and include inputs at both the RADIUS and NMS servers.

Regardless of the platform used (FreeRadius or Cisco Secure ACS), there are four main steps. The first three are for configuring the RADIUS server:

1. Identify the Vendor Specific Attribute (VSA) that names the permission groups
2. Identify the NMS servers that will serve as RADIUS clients
3. Define user ids and assign them to permission groups, information that is included with the VSA

The fourth step is:

4. Configure the NMS server to use the RADIUS server(s).

The following table shows example accounts that are used in this example.

TABLE 8-23 Account Name Examples

User Name	Password	Groups	Notes
Keith_K	knk1knkZ	Admin	Already created on the NMS
John_L	jhl6jhlX	Users	Not already created on the NMS
Paul_M	plh7plhY	Admin	Already created on the NMS

Note: *Admin and Users are the default groups on the NMS available for assignment, though custom groups may be added using the Security Manager on the NMS client. When adding custom groups to a network of NMS servers, the same custom groups must be added to each server individually to be usable by the same set of RADIUS-authenticated users. Refer to "Feature Interactions (RADIUS Server De-activated or Unavailable)" on page 203.*

Note: *Users can optionally be assigned to multiple groups. If so, in some RADIUS servers group names must be separated by commas, contain no white space, and the list must be enclosed by quotation marks. Refer to the server documentation. (The FreeRadius example shows this.)*

8.9.2.1 FreeRadius Example

FreeRadius is a free RADIUS server and is installed on 10.52.18.79.

Note: Downloads and documentation are available at http://freeradius.org/.

To configure for the NMS, begin with cd to /usr/local/etc/raddb and perform the following steps:

Note: For the account Keith_K, the password being defined on RADIUS is different than the password assigned when it had been created on the NMS. Moreover, the group association is being changed from what it had been on the NMS. This will take effect when the user logs in for the first time.

Note: The account John_L had not been created on the NMS, but is defined on the RADIUS server. It will be created on the NMS when the user logs in for the first time.

1. Add the Vendor Specific Attribute (VSA) to the dictionary:

```
VENDOR       Allied-Telesis 207
BEGIN-VENDOR Allied-Telesis
ATTRIBUTE    ATI-avnms-group 1 string
END-VENDOR   Allied-Telesis
```

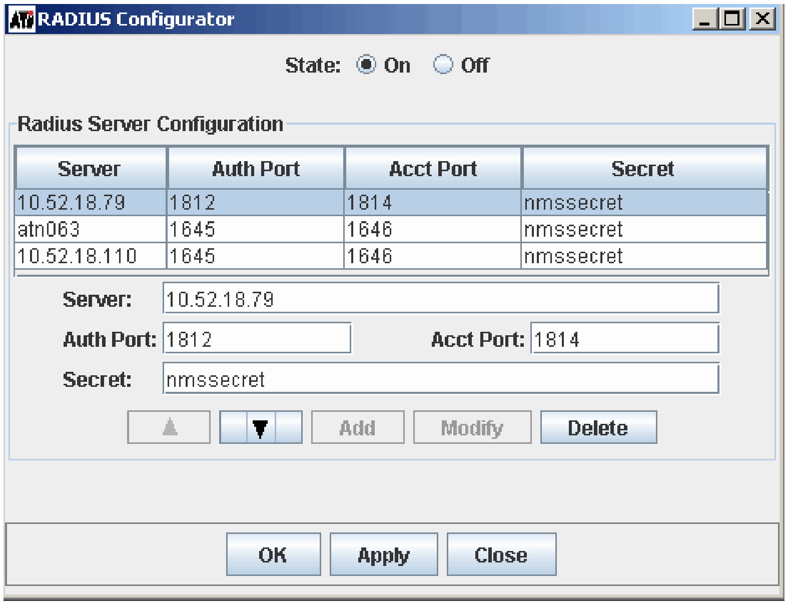
2. Add the RADIUS client (the NMS) to clients.conf

```
client 10.52.18.104 {
    secret      = nmssecret
    shortname   = avnmsuser
    nastype     = other
}
```

3. Add the users to the users file:

```
Keith_K  Auth-Type := Local, User-Password == "knk_radius"
    ATI-avnms-group = "Admin,Users"

John_L   Auth-Type := Local, User-Password == "jhl6jhlX"
    ATI-avnms-group = Users
```

4. Configure the NMS to use this RADIUS server, either by itself or within a list of RADIUS servers. Using the AT_ConfigureRadius tool, assuming the server location is 10.52.18.79, the auth and acct ports are 1812 and 1814 respectively (FreeRADIUS defaults), add the selected line to the NMS configuration, as shown in the following figure.



State: ● On ○ Off

Radius Server Configuration

Server	Auth Port	Acct Port	Secret
10.52.18.79	1812	1814	nmssecret
atn063	1645	1646	nmssecret
10.52.18.110	1645	1646	nmssecret

Server: 10.52.18.79

Auth Port: 1812 Acct Port: 1814

Secret: nmssecret

FIGURE 8-1 Configuring NMS as RADIUS Client

8.9.2.2 Cisco Secure ACS Example

Cisco Secure ACS is a widely-used fee-based RADIUS and TACAC server available from http://www.cisco.com. It comes in platform-specific versions, including various Windows versions.

Note: The NMS is the RADIUS client, which is known as the NAS in the RFC, and is called the AAA Client in Cisco terminology.

Note: Whereas FreeRADIUS defines VSAs in their dictionary *files, Cisco defines VSAs in a RADIUS Vendor/VSA import file.*

Note: Whereas FreeRADIUS defines users and clients in simple configuration files, Cisco uses an extensive web-enabled graphical user interface.

To configure Cisco Secure ACS for the NMS, perform the following:

1. To configure the VSA file, perform the following:
   1. Create a RADIUS Vendor/VSA import file, for example, c:\ACS_Data\allied-telesis.ini, containing the VSA definition:

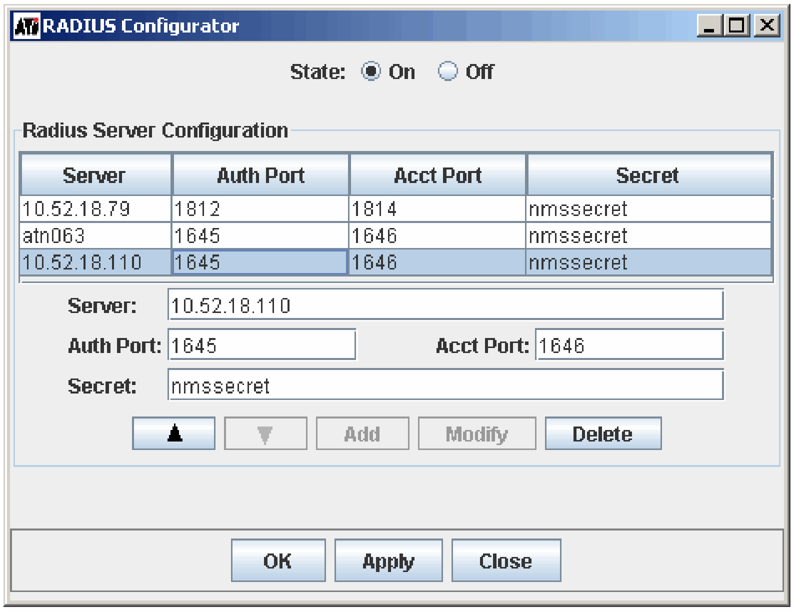
```
[User Defined Vendor]
Name=Allied-Telesis
IETF Code=207
VSA 1=ATI-avnms-group

[ATI-avnms-group]
Type=STRING
Profile=OUT
```

   2. Use CSUtil.exe -listUDV to list available slot numbers and identify one that is unassigned. If none are unassigned, this RADIUS instance has reached its maximum and cannot be used. Either free one or get another server.
2. Add the NMS server as the RADIUS client.
   1. Use CSUtil.exe -addUDV <slot> c:\ACS_Data\allied-telesis.ini to import the VSA file.
   2. Use the Web interface to configure the AAA client (the NMS) and Users with the VSA:
   3. Use “Interface Configuration” to enable RADIUS (Allied-Telesis) for Users.

   4. Use “Network Configuration” to set authentication for the AAA client using RADIUS (Allied-Telesis)

3. Add users and permission groups.
   1. Use “User Configuration” to create the users, assign their passwords, and, at the bottom, enable and assign the VSA (ATI-avnms-group) to the user's permission group(s). Separate multiple group names with commas but do **not** enclose the string with quotation marks.
   2. Select any other relevant options and data fill as necessary.
   3. Be sure all changes are submitted and applied where necessary.

4. Configure the NMS to use this RADIUS server, either by itself or within a list of RADIUS servers. Using the AT_ConfigureRadius tool, assuming the server location is 10.52.18.110, the auth and acct ports are 1645 and 1646 respectively (Cisco defaults), add the selected line to the NMS configuration, as shown in the following figure.



State: ● On ○ Off

Radius Server Configuration

Server	Auth Port	Acct Port	Secret
10.52.18.79	1812	1814	nmssecret
atn063	1645	1646	nmssecret
10.52.18.110	1645	1646	nmssecret

Server: 10.52.18.110

Auth Port: 1645 Acct Port: 1646

Secret: nmssecret

FIGURE 8-2 Configuring NMS as Cisco Secure ACS Client

8.9.3 Feature Interactions (RADIUS Server De-activated or Unavailable)

As shown throughout this section, including in the examples, Admin and Users are the default groups defined on the NMS server, and custom groups may be added using the NMS Security Management feature. The administrator can then choose to include these groups when defining accounts on the RADIUS server.

In most cases, once the administrator has defined these accounts, the RADIUS server is activated, and users log in to the NMS transparently using these defined accounts. The administrator could

1. Change passwords for existing user IDs
2. Change which users belonged to which permission groups.
3. Assign new user IDs and passwords, and associate them with a group or groups

Note: To make these changes, the RADIUS server may need to be restarted. Refer to the appropriate documentation.

However, once the RADIUS NMS client feature has been set up, the following scenarios could occur:

- The customer could de-activate the RADIUS NMS client through the RADIUS Configurator tool.
- The RADIUS server(s), while configured and activated, might not be available.

Refer to "Login behavior RADIUS Server De-activated or not Available" on page 204.

8.9.3.1 Login behavior RADIUS Server De-activated or not Available

When this occurs, the user now must log in with a locally authenticated account, which follows these rules:

- Accounts will belong to the permission groups they had when last used, regardless of whether they were authenticated using RADIUS.
- The passwords are set to what they were the last time **before** RADIUS authentication. This means:
  - If the account was created on the NMS prior to RADIUS authentication, the password reverts to what it was set at on the NMS server.
  - If the account was created on the RADIUS server, the id is still valid, but the default password is the same as the user ID

Using the example accounts listed in "Example Configurations" on page 200 this would mean:

- The user ID Keith_K would revert to the password knk1knkZ, since that is what the pw was set to before RADIUS authentication. However, it would belong to the groups Admin and User, since those were the associated groups defined and last used.
- The user ID John_L would have the password John_L, since the account was created on the RADIUS server.
- The user ID Paul_M would still have a pw of plh7plhY and belong to the Admin group, since it was never created on the RADIUS server.

9. Profile Management

A profile is a set of configuration parameters that is given a unique name. You apply profiles to devices, cards, ports and iMGs in the network.

Profile management includes:

- Configuration - Creating, modifying and deleting profiles.
- Deployment - Applying profiles to network elements.
- Monitoring - Monitoring the network to ensure profiles are applied correctly.

9.1 Network Elements

Each network element has a specific set of profile parameters associated with it. You can create profiles for the following network elements:

Devices	Cards	Ports	iMG/RG Services
iMAP (includes iMAP and SBx3100 devices) Rapier SwitchBlade (includes 9800 devices) AT8900 AlliedWare Plus x200 and x210	POTS MGCP POTS SIP	Etherlike Etherlike DS3 ADSL ADSL Bonded SHDSL VDSL POTS CES-DS1 CES-E1 NTE-DS1 NTE-E1 EPON ONU	General Internet Video Voice CES CES-DS1 Port CES-E1 Port

9.2 Profile Scoping

Profile scoping ensures that profiles and network elements are associated correctly. Profile scoping puts limits both on the network elements that can be associated with a particular profile and the profiles that can be associated a particular network element.

Every element in the network has a name—either an IP address or a DNS name—that uniquely identifies it. When you create a profile, you can enter a value in the **Profile Scoping** field on the **Common** tab that identifies a subset of devices, using the wildcard value * as part of the value. For example, the value 192.168.100.* would include all devices in the network with 192.168.100 in their IP address.

When a profile contains a profile scoping value, then:

- When a profile is part of provisioning, only devices that match the profile scoping value are available.
- When you provision a device to include profiles, only those profiles that match profile scoping will be available.
- When you deploy a profile with profile scoping, only devices within the profile scope will be available.

9.3 Creating a Profile

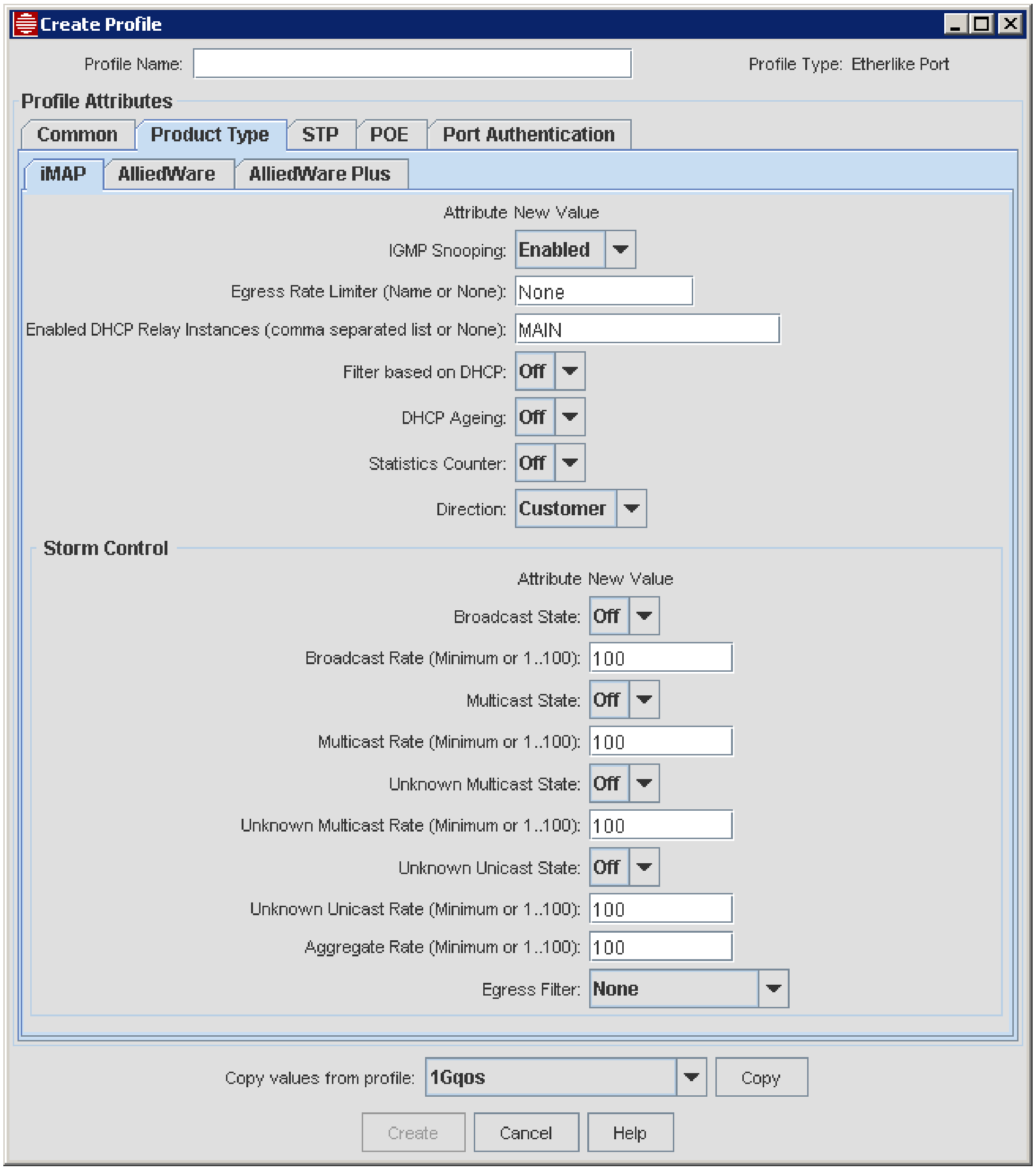
You can create device, card, port and iMG/RG profiles.

1. To create a profile, do one of the following from the **Network Objects** panel:
   - Select **Network Maps > Physical Network** to open the **Physical Network** screen.
   - Select **Network Service Data > Profiles** to open the **Profiles** screen.
2. In the menu bar, go to **Network Services > Profile >** <*profile type*> where <*profile type*> is one of the following:
   - Device Profiles
   - Card Profiles
   - Port Profiles
   - iMG/RG Service Profiles
3. From the menu, select the type of profile you want to create. The **Create Profile** box appears.
4. In the **Profile Name** field, enter a name for the profile. The name can be up to 20 characters long.
5. The **Create Profile** box contains parameters for the selected type of profile.
6. Optionally, you can copy the parameter values from a different profile of the same type to the new profile. This allows you to easily create a new profile that is similar to an existing profile.
7. Once you have entered the profile name and values for the available parameters, click **Create**.

The new profile is stored in the NMS database.

9.3.1 Product Types Tab for Etherlike port

The Etherlike Port profile contains the **Product Type** tab, which includes three sub-tabs: **iMAP**, **AlliedWare** and **AlliedWare Plus**.



Profile Name:

Profile Type: Etherlike Port

Profile Attributes

Attribute	New Value
IGMP Snooping:	Enabled
Egress Rate Limiter (Name or None):	None
Enabled DHCP Relay Instances (comma separated list or None):	MAIN
Filter based on DHCP:	Off
DHCP Ageing:	Off
Statistics Counter:	Off
Direction:	Customer

Storm Control

Attribute	New Value
Broadcast State:	Off
Broadcast Rate (Minimum or 1..100):	100
Multicast State:	Off
Multicast Rate (Minimum or 1..100):	100
Unknown Multicast State:	Off
Unknown Multicast Rate (Minimum or 1..100):	100
Unknown Unicast State:	Off
Unknown Unicast Rate (Minimum or 1..100):	100
Aggregate Rate (Minimum or 1..100):	100
Egress Filter:	None

Copy values from profile: 1Gqos

FIGURE 9-1 Create Profile for Ethernet Port - Product Type Tab

9.3.2 Configuring Storm Control

Storm control is available on SBx3100 devices. Storm control uses ingress and egress functionality to control broadcast, known and unknown multicast, and unknown unicast traffic in the system. Using storm control, you can protect the quality of service by limiting the percentage of inbound and outbound multi-destination traffic in the system. Storm control must be set in profiles and cannot be modified on individual devices.

You set storm control rates on ingress interfaces as a percentage of the actual interface line speed. If the line speed changes, the actual rate limit will change as a percentage of the new line speed. For example, on a 1G interface, a 1% limit is enforced as 10M. If the interface auto-negotiates up at 100M , then the 1% limit is enforced as 1M.

The GE40CSFP and GE40RJ cards support a separate rate limit for each traffic type. The GE24SFP, XE4, XE6SFP, GE24POE and GE24RJ cards support one rate limit for all traffic types. This is represented by the **Aggregate Rate** field in the profile box. The aggregate rate represents the total allowed rate for all traffic types that have storm control enabled.

Caution: Most Ethernet services rely heavily on the flooding of broadcast and unknown unicast packets. Filtering egress traffic may cause service outages.

To enable storm control in a profile:

1. In the **Network Objects** panel, select **Network Service Data > Profiles** to open the **Profiles** screen.
2. Do one of the following:
   - To create a new profile, in the menu bar, go to **Network Services > Profile > Port Profiles > Create Etherlike Port**.
   - To modify an existing profile, select the profile, right-click and select **View Profile**.
3. Select the **Product Type** tab.
4. Select the **iMAP** tab if it is not already selected.
5. Under **Storm Control**, enter values for the following fields:

Field	Values	Notes
Broadcast State	**On** - Enables storm control on ingress interfaces for broadcast traffic. **Off** - Disables storm control on ingress interfaces for broadcast traffic.	
Broadcast Rate	**Minimum** - Sets the percentage of the operational bandwith of the interfaces that will be usable by broadcast traffic to as close to zero as the hardware supports. **1-100** - The maximum percentage of the operational bandwith of the interfaces that will be usable by broadcast traffic. Any traffic that exceeds this limit is discarded.	This field applies to GE40CSFP and GE40RJ cards.

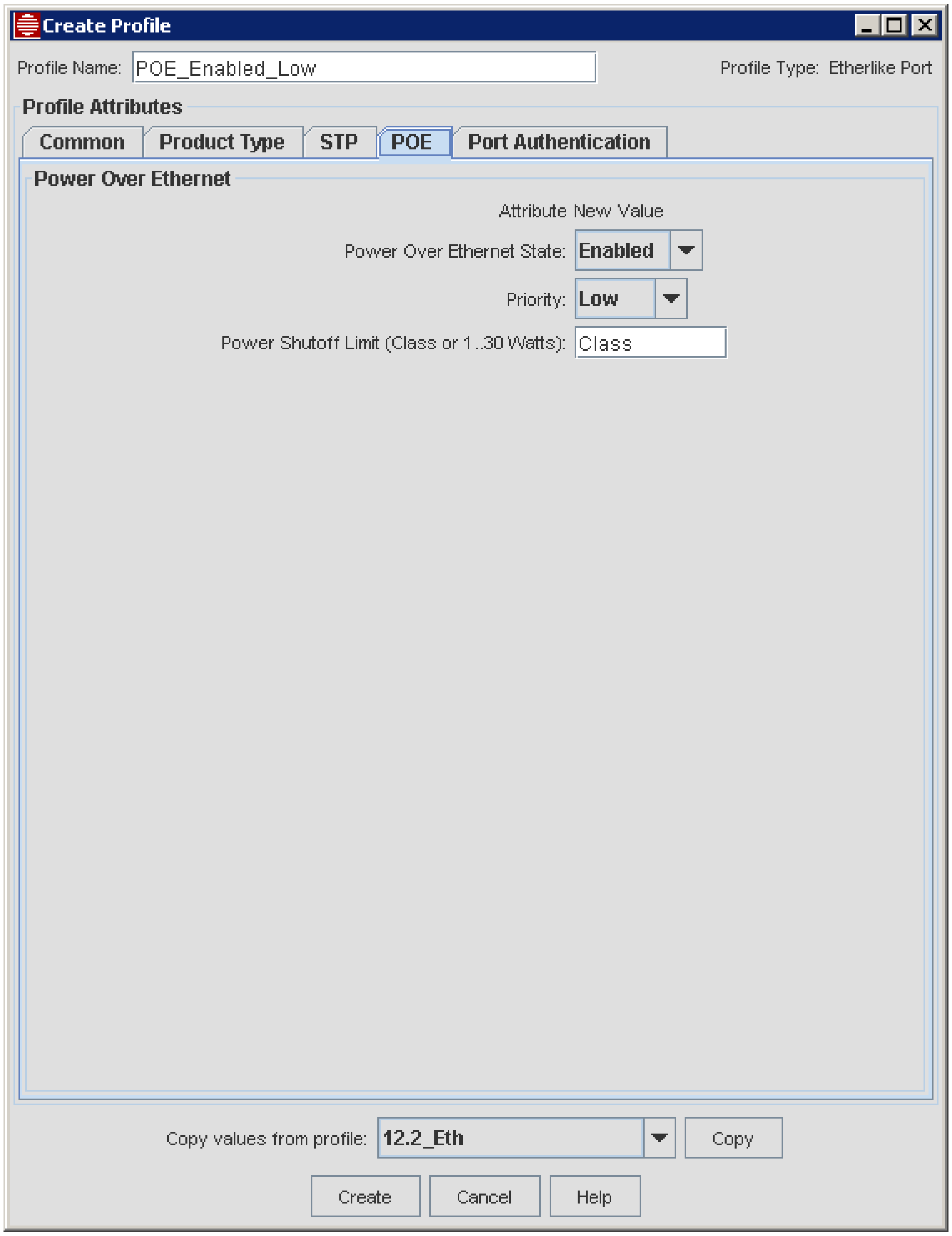
Field	Values	Notes
Multicast State	**On** - Enables storm control on ingress interfaces for both known and unknown multicast traffic. **Off** - Disables storm control on ingress interfaces for known and unknown multicast traffic.	**Multicast State** and **Unknown Multicast State** cannot be enabled at the same time Only one of the two can be enabled at one time. For example, if Unknown Multicast is enabled, Multicast will automatically become disabled when creating the profile and vice versa. If Unknown Multicast is enabled and Multicast is disabled, unknown multicast traffic will no longer have rate limits applied (storm control will be disabled). Unknown Multicast is only supported on GE40CSFP and GE40RJ cards. Unknown Multicast will remain disabled for GE24SFP, GE24POE, GE2RJ, XE4 and XE6SFP cards.
Multicast Rate	**Minimum** - Sets the percentage of the operational bandwith of the interfaces that will be usable by multicast traffic to as close to zero as the hardware supports. **1-100** - The maximum percentage of the operational bandwith of the interfaces that will be usable by multicast traffic. Any traffic that exceeds this limit is discarded.	This field applies to GE40CSFP and GE40RJ cards.
Unknown Multicast State	**On** - Enables storm control on ingress interfaces for unknown multicast traffic only. **Off** - Disables storm control on ingress interfaces for unknown multicast traffic.	**Multicast State** and **Unknown Multicast State** cannot be enabled at the same time Only one of the two can be enabled at one time. For example, if Unknown Multicast is enabled, Multicast will automatically become disabled when creating the profile and vice versa. If Unknown Multicast is enabled and Multicast is disabled, unknown multicast traffic will no longer have rate limits applied (storm control will be disabled). Unknown Multicast is only supported on GE40CSFP and GE40RJ cards. Unknown Multicast will remain disabled for GE24SFP, GE24POE, GE2RJ, XE4 and XE6SFP cards.

Field	Values	Notes
Unknown Multicast Rate	**Minimum** - Sets the percentage of the operational bandwith of the interfaces that will be usable by unknown multicast traffic to as close to zero as the hardware supports. **1-100** - The maximum percentage of the operational bandwith of the interfaces that will be usable by unknown multicast traffic. Any traffic that exceeds this limit is discarded.	This field applies to GE40CSFP and GE40RJ cards.
Unknown Unicast State	**On** - Enables storm control on ingress interfaces for unknown unicast traffic. **Off** - Disables storm control on ingress interfaces for unknown unicast traffic.	
Unknown Unicast Rate	**Minimum** - Sets the percentage of the operational bandwith of the interfaces that will be usable by unknown unicast traffic to as close to zero as the hardware supports. **1-100** - The maximum percentage of the operational bandwith of the interfaces that will be usable by unknown unicast traffic. Any traffic that exceeds this limit is discarded.	This field applies to GE40CSFP and GE40RJ cards.
Aggregate Rate	**Minimum** - Sets the percentage of the operational bandwith of the interfaces that will be usable by all traffic types that have storm control enabled to as close to zero as the hardware supports. **1-100** - The maximum percentage of the operational bandwith of the interfaces that will be usable by all traffic types that have storm control enabled. Any traffic that exceeds this limit is discarded.	This field applies to GE24SFP, XE4, XE6SFP, GE24POE and GE24RJ cards.
Egress Filter	**None** - Egress traffic filtering is disabled. **Broadcast** - Enables egress filtering for broadcast traffic. **Unknown Unicast** - Enables egress filtering for unknown unicast traffic. **All** - Enables egress filtering for all broadcast and unknown unicast traffic.	Most Ethernet services rely heavily on the flooding of broadcast and unknown unicast packets. Filtering egress traffic may cause service outages.

6. Click **Create** or **Modify** to save the settings to the profile.

9.3.3 Etherlike Profile for GE24POE includes POE

To configure the GE24POE port on the SBx3100, the POE tab is included with the Etherlike Profile, as shown in the following figure.



Profile Name: POE_Enabled_Low

Profile Type: Etherlike Port

Profile Attributes

Power Over Ethernet

Attribute New Value

Power Over Ethernet State: Enabled

Priority: Low

Power Shutoff Limit (Class or 1..30 Watts): Class

Copy values from profile: 12.2_Eth

FIGURE 9-2 Etherlike Profile for POE

The three values to be filled in are:

- Power Over Ethernet State - Whether to enable or disable the feature
- Priority - Ports with lower priority will stop being powered when the system cannot allocate enough power to all ports.
- Power Shutoff Limit - Power will be cut off if it exceeds the set threshold

9.3.4 Etherlike Profile for SBx3100 Ports Includes Port Authentication

For ports on the SBx3100, there is also the Port Authentication feature. Refer to "Port Authentication (802.1x)" on page 688.

9.4 Viewing and Modifying Profiles

To view profiles, in the **Network Objects** panel, select **Network Service Data > Profiles** to open the **Profiles** screen.

The profiles can be viewed like other attributes, so they can be sorted, scrolled, and have a search function.

To view or modify the details of the profile, the user can right click the profile and select View Profile, or double-click the profile. The **Modify Profile** box appears, and when the user changes any parameter the **Modify** button is activated.

Note: At this point, the profiles have not been deployed, and so changing any values has no effect on what parameter values are actually used on any devices or ports. The relationship between deployed profiles and the changing of parameter values is discussed later.

Note: Creating and deploying profiles for the EPON and ONU requires particular attention since the user must understand the attributes of the EPON and ONU interface policies.

9.5 Deleting a Profile

The user can delete a profile if it is not being used (deployed) on a device or port. To delete a profile, right click on the profile and select Delete Profile. A confirmation window confirms the deletion.

Note: This operation will fail if there are any objects (devices or ports) in the network that are currently using one of the profiles to be deleted. If there are objects currently using one of the profiles, the user can apply some other Profile (such as a default profile) to those objects and then successfully delete the profile.

9.6 Deploying a Profile

When you deploy a profile, the configuration values set in the profile are applied to a set of devices or ports in the network.

When you apply device profiles to devices, you can select devices to:

- Apply the device profile to a selected list of devices
- Apply the device profile to all devices that are currently using a particular device profile
- Apply the device profile to all devices in a particular network/sub-network

When you apply port profiles to ports, you can select ports across multiple device types. You can:

- Apply the port profile to all ports of the correct type on a selected list of devices
- Apply the port profile to ports of the correct type on a selected list of devices that are currently using a particular port profile
- Apply the port profile to all ports of the correct type on all devices that are currently using a particular port profile
- Apply the port profile to a selected set of ports of the correct type on selected devices where the set of ports can be different for each of the selected devices
- Apply the port profile to all ports of the correct type on the selected list of devices that are not currently configured to use a profile or are using the default profile
- Apply the port profile to the auto-provisioning profile of a device

To deploy a profile:

1. In the **Network Objects** panel, go to **Network Service Data > Profiles**.
2. In the **Profiles** window, select the profile you want to deploy.

3. Do one of the following:
   - Right-click and select **Deploy Profile**.
   - From the menu, go to **Profile > Deploy Profile**.

   The Deploy Profile box for the type of profile selected appears.

To fill out the Deploy Profile box, follow these steps:

1. Enter the device or port selection method (one of the selection methods described in bullet lists at the top of this section).
2. Depending on the selection method chosen, select the devices and/or ports on which to apply the profile.

Note: If the Profile Scoping field was used in filling out the Profile, only those devices that match the Profile Scoping are available.

3. Click **Deploy**.
4. An AlliedView NMS Task Details window is displayed indicating the progress of the Profile Deployment task as the devices in the network are updated.
5. The “Node” or “Configured Ports” tables will be updated to indicate that the selected devices or ports are now using the selected Profile. (This is part of Profile Monitoring, described in "Profile Monitoring" on page 215.)

9.7 Redeploying a Profile

There are times when you need to re-synchronize the parameters stored in the Profile on the NMS with the configuration of the actual devices or ports in the network. This could be needed after a change is made to the Profile, or when the user wants to reset any temporary changes made to individual ports in the network back to the Profile configuration. To re-apply or re-deploy a profile to the network, follow these steps:

1. Bring up the Profile Deployment window for a device or port.
2. To re-deploy Port Profiles select **Apply to ports with Profile** port selection method.
3. To re-deploy Device Profiles select **Apply to devices with Profile** device selection method.
4. Select the current profile.
5. Press the **Deploy** button.
6. The NMS will start a Task to reset all the parameters on the appropriate device(s) or port(s) to match those defined in the Profile.

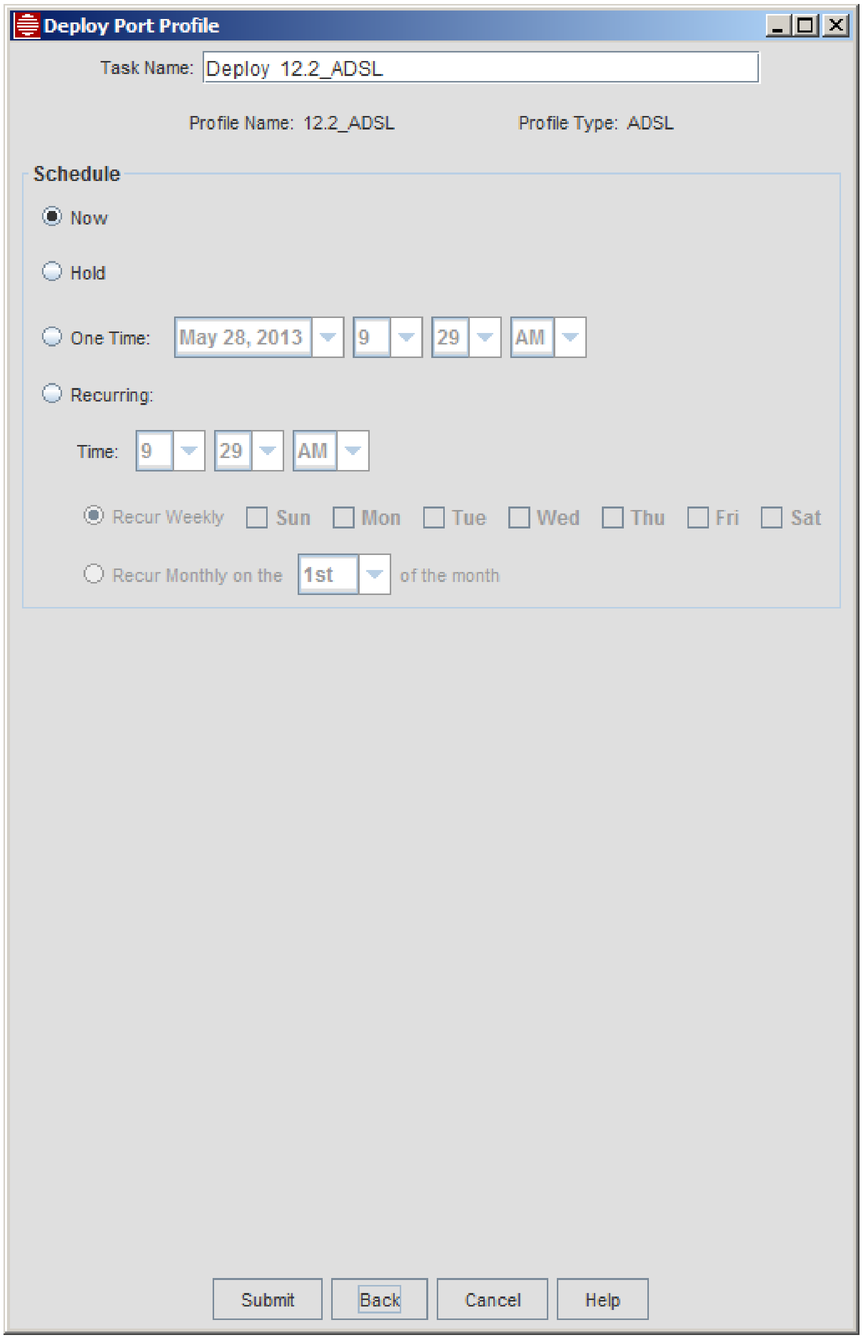
Note: The NMS will only set parameters where the value on the device differs for the value in the Profile.

9.8 Scheduling Deployment of a Profile

There are situations where a Profile should be deployed at a particular time in the future (such as pending service activation) or at regular intervals (such as switching back and forth between two Profiles based on time of day or day of week). To schedule the deployment of a profile follow these steps:

1. Sets up a profile deployment.
2. Instead of pressing the **Deploy** button, press the **Next** button to bring up the scheduling window.
3. Select One Time schedule or Recurring schedule and the appropriate parameters for each.
4. Press the **Finish** button to submit the request to the NMS scheduler.
5. At the specified time(s), the NMS deploys the Profile.

Note: The scheduling mechanism will be the same one as used by the Device Backup/Restore and Software Download applications.



Task Name: Deploy 12.2_ADSL

Profile Name: 12.2_ADSL Profile Type: ADSL

● Now

○ Hold

○ One Time: May 28, 2013 9 29 AM

○ Recurring:

Time: 9 29 AM

● Recur Weekly □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

○ Recur Monthly on the 1st of the month

FIGURE 9-3 Deploy Port Profile Form - Scheduling

9.9 Deploying Changes to a Profile

When you modify a profile, any device or port in the network using that profile will no longer be consistent with the profile settings. When modifying a Profile on the NMS, the NMS will allow the user to have the NMS automatically push the changes in the profile to the objects (devices or ports) in the network to which the profile had been applied. Follow these steps:

1. Modify a profile as defined in "Viewing and Modifying Profiles" on page 212.

2. The NMS prompts the user whether the changes should be deployed to the objects (devices or port) in the network currently using that Profile.

3. If yes, the profile will be redeployed.

9.10 Profile Monitoring

Profile monitoring is the process tracking the Profiles being used by objects in the network. It also includes the tracking of whether the individual settings of the object are consistent with the parameters defined in the Profile that was applied to it. The settings can deviate from the Profiles over time as the devices are manipulated through non-AlliedView NMS methods (such as using the CLI directly). To better manage the Profiles, the NMS monitors the Profile to port and device associations in the network.

9.10.1 Viewing Profile to Port Associations

The user can view a list of ports that indicate which Port Profile each of the ports is currently using. This view will also indicate whether the parameters set on the port are still consistent with the Port Profile defined on the NMS. Perform the following steps:

Note: The table used to display the Port Profile usage will be that same table that indicates the Customer ID associated with each port. This panel is named "Configured Ports".

1. Select the "Ports" panel under the Network Inventory Object.

2. The Ports panel will contain a table that lists the configured ports in the network. The columns in the table include the device/slot/port of the port, the customer id associated with the port, and the Port Profile associated with the port with an indication as to whether the port configuration is in sync with the Port Profile settings defined in the NMS.

9.10.2 Viewing Profile to Device Associations

The user can view a list of devices that indicate which Device Profile each of the devices is currently using. This view will also indicate whether the parameters set on the device are still consistent with the Device Profile defined on the NMS.

1. Select the "Profile Association" panel under "Nodes".

2. The Profile Association panel will contain a table that lists the devices in the network. The columns in the table include the name, type, ip address, and Device Profile with an indication whether the device configuration is in sync with the Device Profile settings defined in the NMS.

9.11 Keeping the Profile Parameters and Ports/Devices in Sync

Over time, either through the NMS or directly with the devices, the user can make changes to the devices or ports so that they are no longer in sync with the configuration defined in the Profiles. The NMS must discover this discrepancy and keep the Ports and Profile Association Panels up to date.

- To check for changes made directly to the device that affect the device level configuration, the NMS rediscovery process compares the values on the device with the Device Profile that was applied to it and update the Node table accordingly. This means that a change on the device will go undetected by the NMS only until the next rediscovery of the device is automatically invoked by the NMS.
- To check for changes made directly to the device that affect the port configuration, the NMS rediscovery process will compare the port configuration on the device with the Port Profile that was applied to it and update the Configured Ports table accordingly. This means that a change on the device will go undetected by the NMS only until the next rediscovery of the device is automatically invoked by the NMS.
- For changes made through the NMS, the applications that make the changes to a device or port will update the NMS tables immediately.

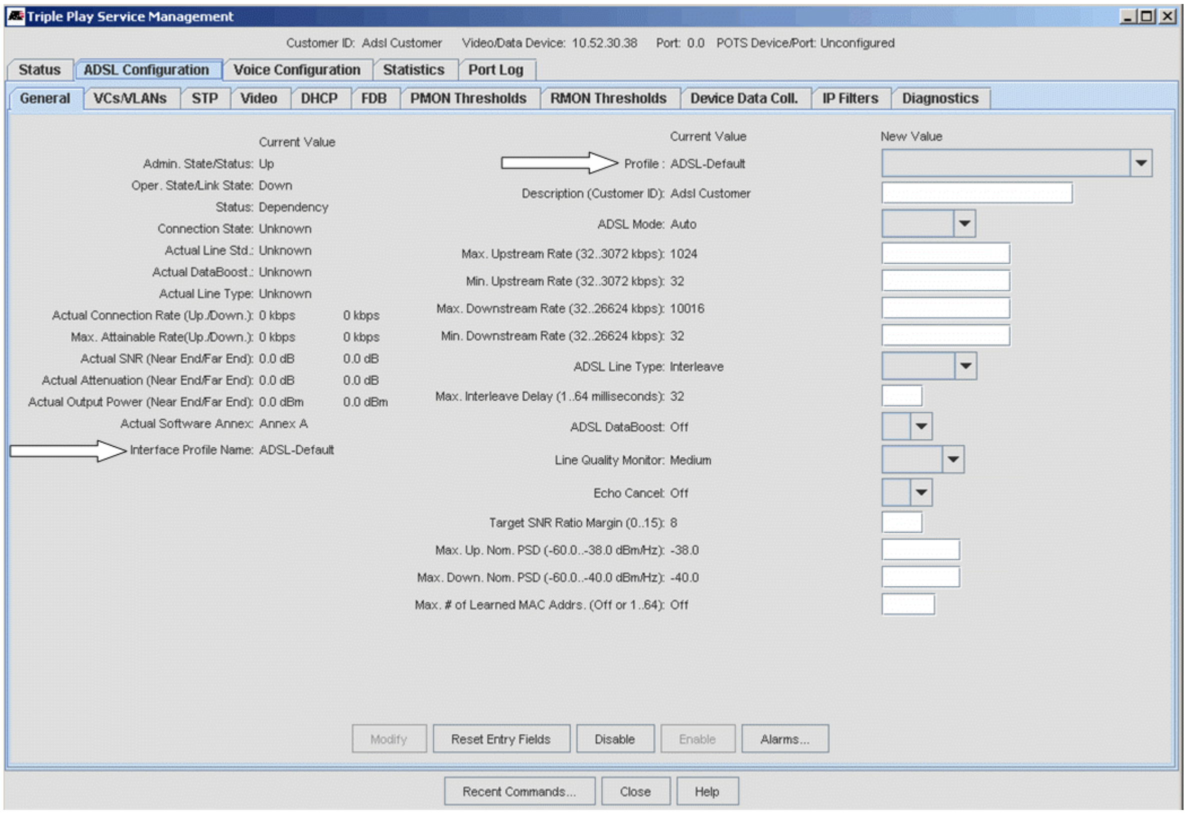
Note: *When a profile is out of sync with what has been defined on the device, a "*" is next to the profile name in the Profile column of the Port or Device table.*

9.12 Coordination of External and NMS Profiles

As described above, the *Allied*View NMS profiles operate at the network service level; a profile is created for a card type or port type, and can then be applied to multiple interfaces over multiple devices. Moreover, the profiles include a more global set of attributes, such as traffic and performance management attributes. Finally, the profiles are filled out using pull-down menus and GUIs, ensuring there is less chance of error.

When the NMS sets the port attributes by deploying an NMS profile, the SHOW INTERFACE command on the iMAP displays the NMS profile name that has been applied as an **External Profile** name. Moreover, if at the NMS a port is deprovisioned, the iMAP output for External Profile is set to None.

At the NMS, when an iMAP port is displayed, the current value of the External Profile name will be displayed at or near the bottom of the view-only attributes, labeled "Interface Profile Name". Normally this name will match the Profile name deployed by the NMS (displayed upper right). Refer to the following figure.



Customer ID: Adsl Customer Video/Data Device: 10.52.30.38 Port: 0.0 POTS Device/Port: Unconfigured

	Current Value	
Admin. State/Status:	Up	
Oper. State/Link State:	Down	
Status:	Dependency	
Connection State:	Unknown	
Actual Line Std.:	Unknown	
Actual DataBoost.:	Unknown	
Actual Line Type:	Unknown	
Actual Connection Rate (Up./Down.):	0 kbps	0 kbps
Max. Attainable Rate(Up./Down.):	0 kbps	0 kbps
Actual SNR (Near End/Far End):	0.0 dB	0.0 dB
Actual Attenuation (Near End/Far End):	0.0 dB	0.0 dB
Actual Output Power (Near End/Far End):	0.0 dBm	0.0 dBm
Actual Software Annex:	Annex A	
Interface Profile Name:	ADSL-Default	

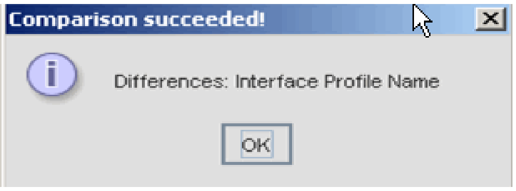
	Current Value	New Value
Profile :	ADSL-Default	
Description (Customer ID):	Adsl Customer	
ADSL Mode:	Auto	
Max. Upstream Rate (32..3072 kbps):	1024	
Min. Upstream Rate (32..3072 kbps):	32	
Max. Downstream Rate (32..26624 kbps):	10016	
Min. Downstream Rate (32..26624 kbps):	32	
ADSL Line Type:	Interleave	
Max. Interleave Delay (1..64 milliseconds):	32	
ADSL DataBoost:	Off	
Line Quality Monitor:	Medium	
Echo Cancel:	Off	
Target SNR Ratio Margin (0..15):	8	
Max. Up. Nom. PSD (-60.0..-38.0 dBm/Hz):	-38.0	
Max. Down. Nom. PSD (-60.0..-40.0 dBm/Hz):	-40.0	
Max. # of Learned MAC Addrs. (Off or 1..64):	Off	

FIGURE 9-4 ADSL Details - NMS and Interface Profile

Whenever a profile is deployed by the NMS to the port, the Interface Profile Name will be set to the port Profile name. Note that there is no other way to change the Interface Profile Name via the NMS. If for whatever reason the names do not match, for example someone changes the external profile name on the device using the CLI, the port profile name (upper right) will be marked with an asterisk. Normally this will only be detected during discovery, when the NMS automatically performs port-profile comparison.

Note: *The administrator must therefore be aware that if the External Profile Name is changed at the CLI, there will be no notification of this at the NMS until the device is (re)discovered.*

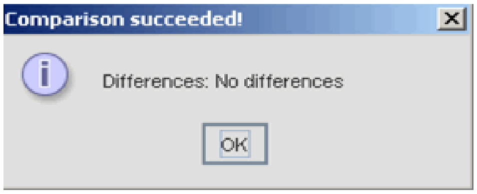
When a port is activated from the Ports Inventory table, a message such as the following will be displayed if the profile name and external profile name do not match exactly:


Comparison succeeded!

Differences: Interface Profile Name

FIGURE 9-5 NMS and External Profile Name do not Match

When the names match and no other parameter mismatches, the usual message is displayed:


Comparison succeeded!

Differences: No differences

FIGURE 9-6 NMS and External Profile Name Match

9.13 ADSL G.Bond Creation and use of Profiles

The NMS supports G.bond (ITU G.998) for ADSL interfaces.

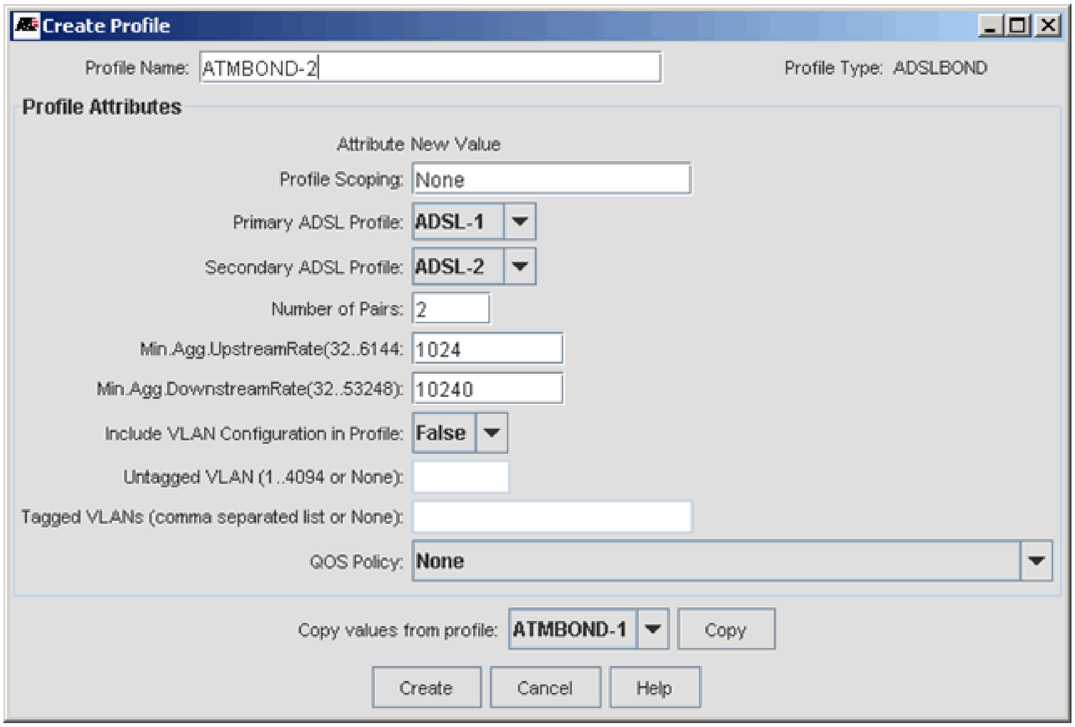
To provision this, there is the profile called ADSLBOND, and it contains references to two regular ADSL profiles, referred to as the Primary and Secondary profiles. (Refer to Figure 9-7.)

The NMS supports two ADSL interfaces: Primary and Secondary. One acts as the primary (root) port and all other ports are secondary.

Normally, the same ADSL profile is used for both the Primary and Secondary profile, so when the Primary is selected the Secondary defaults to the same profile. Additional fields include the minimum upstream/downstream rates.

Since Tagged and Untagged VLANs can be attached to the ETH interface of the bond, the referenced ADSL profiles must **not** contain VLAN information. Therefore, ADSL profiles that are referenced by an ADSL-BOND profile must have their “Include VLAN Configuration” value disabled. The QOS Policy parameter is treated similarly; it must be set to NONE in ADSL profiles that are referenced by ATM-BOND profiles.

During creation of an ADSL-BOND profile, if no appropriate ADSL profiles can be found, a window will popup explaining these requirements and then the profile window will close.



Create Profile

Profile Name: ATMBOND-2

Profile Type: ADSLBOND

Profile Attributes

Attribute	New Value
Profile Scoping:	None
Primary ADSL Profile:	ADSL-1
Secondary ADSL Profile:	ADSL-2
Number of Pairs:	2
Min.Agg.UpstreamRate(32..6144:	1024
Min.Agg.DownstreamRate(32..53248):	10240
Include VLAN Configuration in Profile:	False
Untagged VLAN (1..4094 or None):	
Tagged VLANs (comma separated list or None):	
QOS Policy:	None

Copy values from profile: ATMBOND-1

FIGURE 9-7 ADSL-Bond Profile

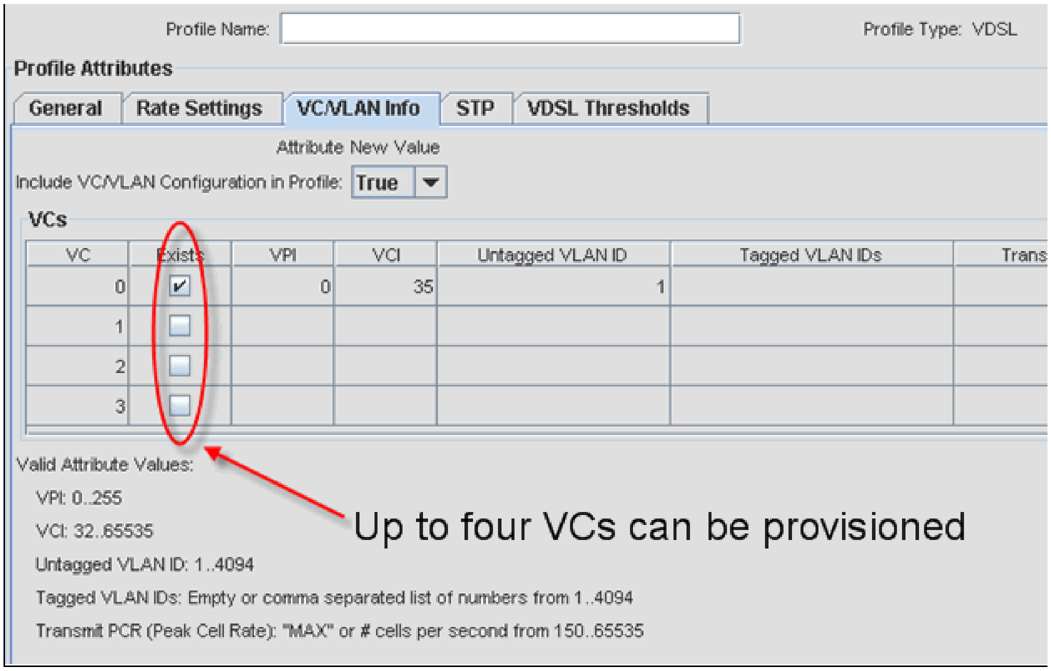
9.14 Multiple VC Support on VDSL Port

On the iMAP, you can provision multiple VCs for the VDSL A/B cards in ADSL or VDSL mode over ATM. Like the ADSL24A/B, the VDSL24A/B cards support the provisioning of VCs as long as the port is running ATM in either ADSL or VDSL mode. Up to 4 AAL5 VCs per ATM interface can be configured with different VPI/VCI pairs. Moreover, the same rules apply for the VDSL24A/B card as with the other ADSL cards that support multi-VCs (sub-interface zero is created by default and cannot be destroyed).

Messages are added to the GUI so that the administrator is informed that when the transport mode is set to PTM, VCs cannot be provisioned. This and the other GUI changes are explained below.

9.14.1 Create/Modify VDSL Profile

The Create VDSL Profile is changed so that when the transport mode is set to ATM, there is the option to data fill up to four VCs. (VC 0 always exists and cannot be deleted.) Refer to the following figure.



Profile Name:

Profile Type: VDSL

Profile Attributes

Attribute New Value

Include VC/VLAN Configuration in Profile: True

VCs

VC	Exists	VPI	VCI	Untagged VLAN ID	Tagged VLAN IDs	Trans
0	☑	0	35	1		
1	□					
2	□					
3	□					

Valid Attribute Values:

VPI: 0..255

VCI: 32..65535

Untagged VLAN ID: 1..4094

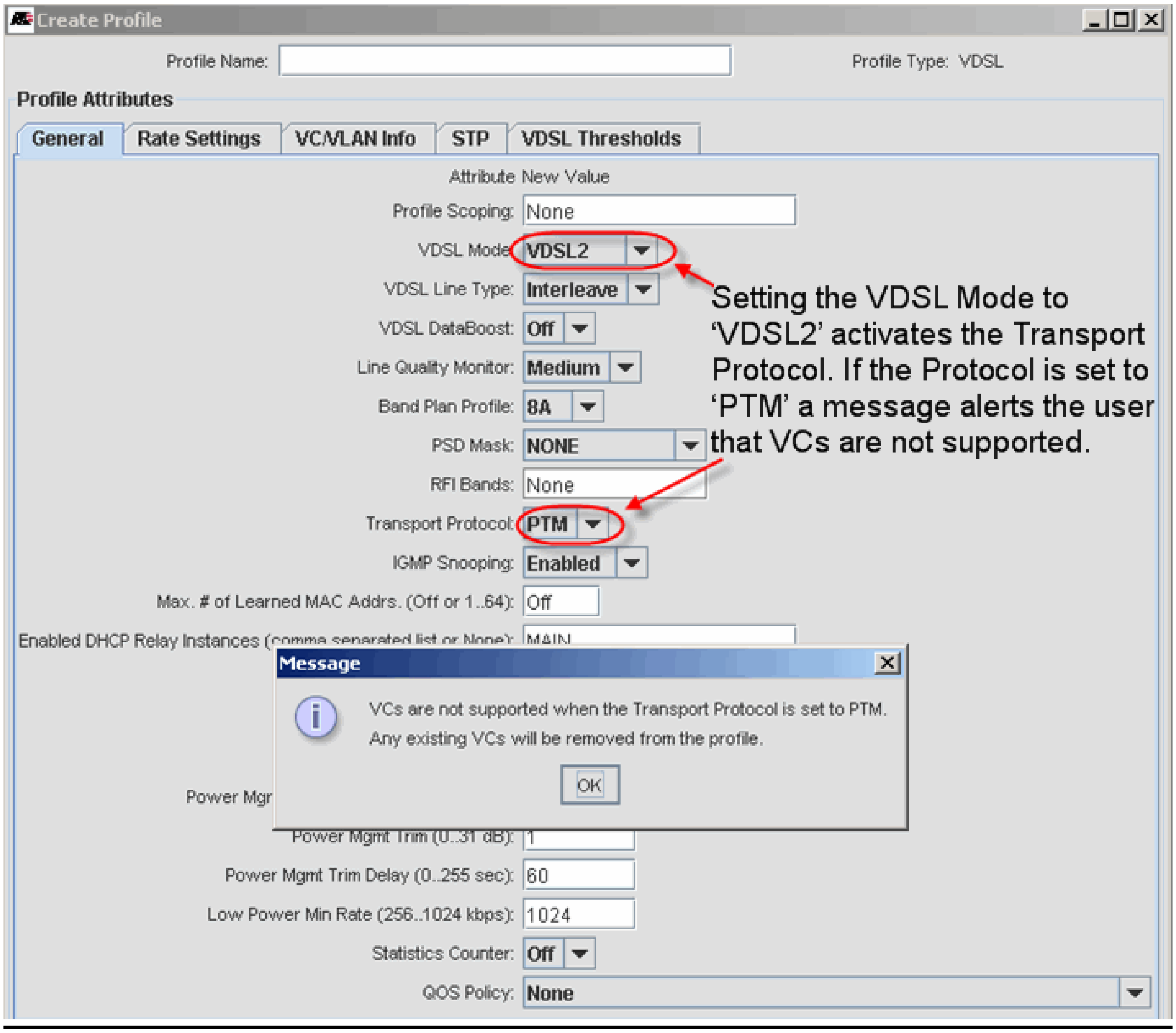
Tagged VLAN IDs: Empty or comma separated list of numbers from 1..4094

Transmit PCR (Peak Cell Rate): "MAX" or # cells per second from 150..65535

Up to four VCs can be provisioned

FIGURE 9-8 VDSL Profile - VCs in ATM Mode

When the Transport Protocol is set to PTM the user will receive a warning, as shown in the following figure.



Create Profile

Profile Name:

Profile Type: VDSL

Profile Attributes

Attribute	New Value
Profile Scoping:	None
VDSL Mode:	VDSL2
VDSL Line Type:	Interleave
VDSL DataBoost:	Off
Line Quality Monitor:	Medium
Band Plan Profile:	8A
PSD Mask:	NONE
RFI Bands:	None
Transport Protocol:	PTM
IGMP Snooping:	Enabled
Max. # of Learned MAC Addrs. (Off or 1..64):	Off
Enabled DHCP Relay Instances (comma separated list or None):	MAIN
Power Mgr	
Power Mgmt Trim (0..31 dB):	1
Power Mgmt Trim Delay (0..255 sec):	60
Low Power Min Rate (256..1024 kbps):	1024
Statistics Counter:	Off
QOS Policy:	None

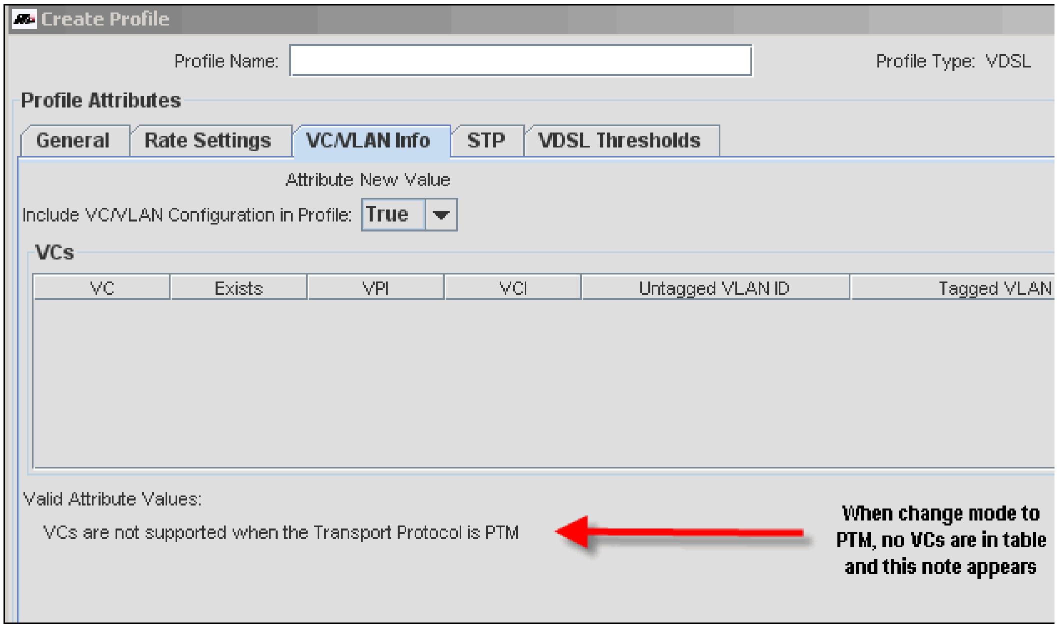
Message

VCs are not supported when the Transport Protocol is set to PTM.
Any existing VCs will be removed from the profile.

Setting the VDSL Mode to 'VDSL2' activates the Transport Protocol. If the Protocol is set to 'PTM' a message alerts the user that VCs are not supported.

FIGURE 9-9 Setting the Transport Protocol to PTM (VDSL Port)

After clicking OK, you can go to the VC/VLAN tab and see that there are no VCs, as shown in the following figure.



Profile Name:

Profile Type: VDSL

Attribute New Value

Include VC/VLAN Configuration in Profile: True

VC	Exists	VPI	VCI	Untagged VLAN ID	Tagged VLAN

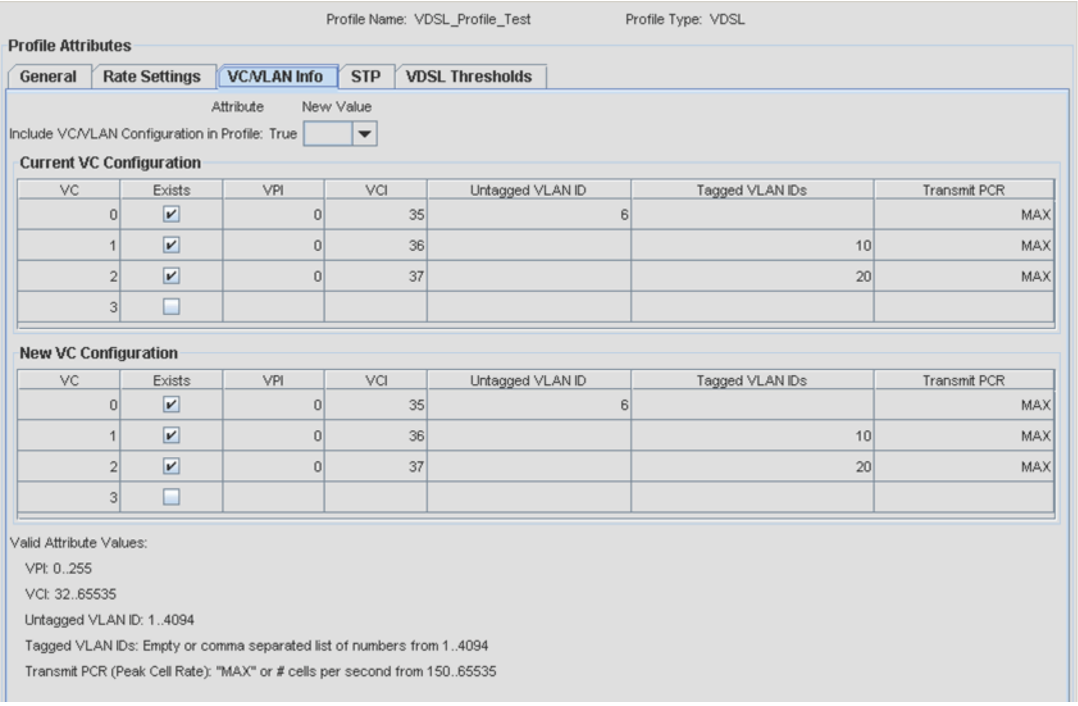
Valid Attribute Values:

VCs are not supported when the Transport Protocol is PTM

When change mode to PTM, no VCs are in table and this note appears

FIGURE 9-10 VC/VLAN Tab when VDSL in PTM Mode

The Modify VDSL Profile VC/VLAN tab has two tables, one for the current settings in the profile, and one for putting in changes. This has the same behavior as the Create VDSL Profile, in that the Transport protocol settings alter these tables. Refer to the following figures.



Profile Name: VDSL_Profile_Test

Profile Type: VDSL

Attribute New Value

Include VC/VLAN Configuration in Profile: True

Current VC Configuration

VC	Exists	VPI	VCI	Untagged VLAN ID	Tagged VLAN IDs	Transmit PCR
0	☑	0	35	6		MAX
1	☑	0	36		10	MAX
2	☑	0	37		20	MAX
3	☐					

New VC Configuration

VC	Exists	VPI	VCI	Untagged VLAN ID	Tagged VLAN IDs	Transmit PCR
0	☑	0	35	6		MAX
1	☑	0	36		10	MAX
2	☑	0	37		20	MAX
3	☐					

Valid Attribute Values:

VPI: 0..255

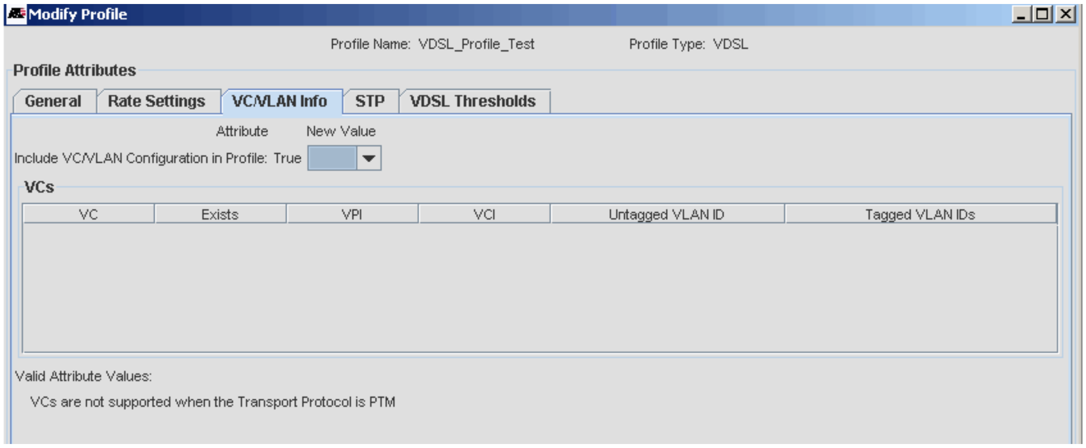
VCI: 32..65535

Untagged VLAN ID: 1..4094

Tagged VLAN IDs: Empty or comma separated list of numbers from 1..4094

Transmit PCR (Peak Cell Rate): "MAX" or # cells per second from 150..65535

FIGURE 9-11 Modify Profile before Mode set to PTM



Profile Name: VDSL_Profile_Test Profile Type: VDSL

	Attribute	New Value
Include VC/VLAN Configuration in Profile:	True	

VCs

VC	Exists	VPI	VCI	Untagged VLAN ID	Tagged VLAN IDs

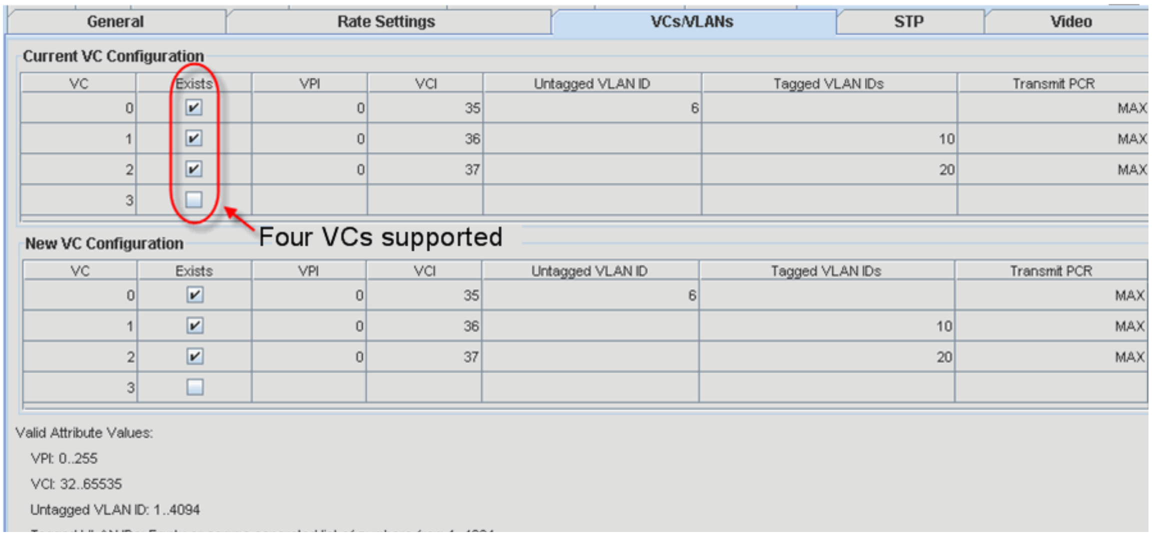
Valid Attribute Values:

VCs are not supported when the Transport Protocol is PTM

FIGURE 9-12 Modify Profile after Mode set to PTM

9.14.2 Triple Play Service Management Form

The Triple Play Service Management form, VDSL Configuration tab also reflects the multiple-VC provisioning, as shown in the following figures.



Current VC Configuration

VC	Exists	VPI	VCI	Untagged VLAN ID	Tagged VLAN IDs	Transmit PCR
0	☑	0	35	6		MAX
1	☑	0	36		10	MAX
2	☑	0	37		20	MAX
3	□					

New VC Configuration

VC	Exists	VPI	VCI	Untagged VLAN ID	Tagged VLAN IDs	Transmit PCR
0	☑	0	35	6		MAX
1	☑	0	36		10	MAX
2	☑	0	37		20	MAX
3	□					

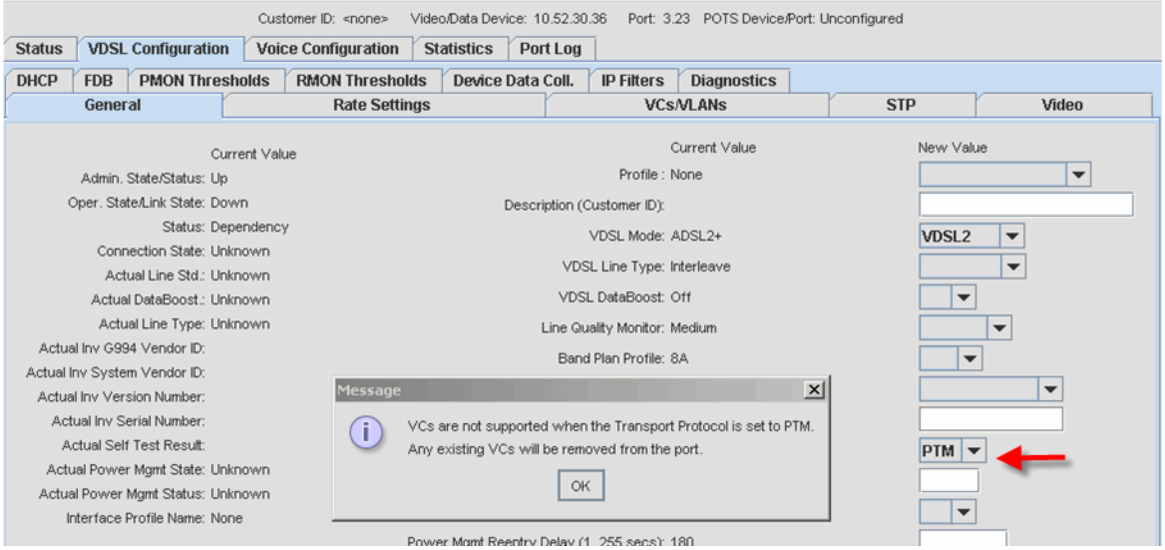
Valid Attribute Values:

VPI: 0..255

VCI: 32..65535

Untagged VLAN ID: 1..4094

FIGURE 9-13 VDSL Service Management Form - ATM Mode



Customer ID: <none> Video/Data Device: 10.52.30.36 Port: 3.23 POTS Device/Port: Unconfigured

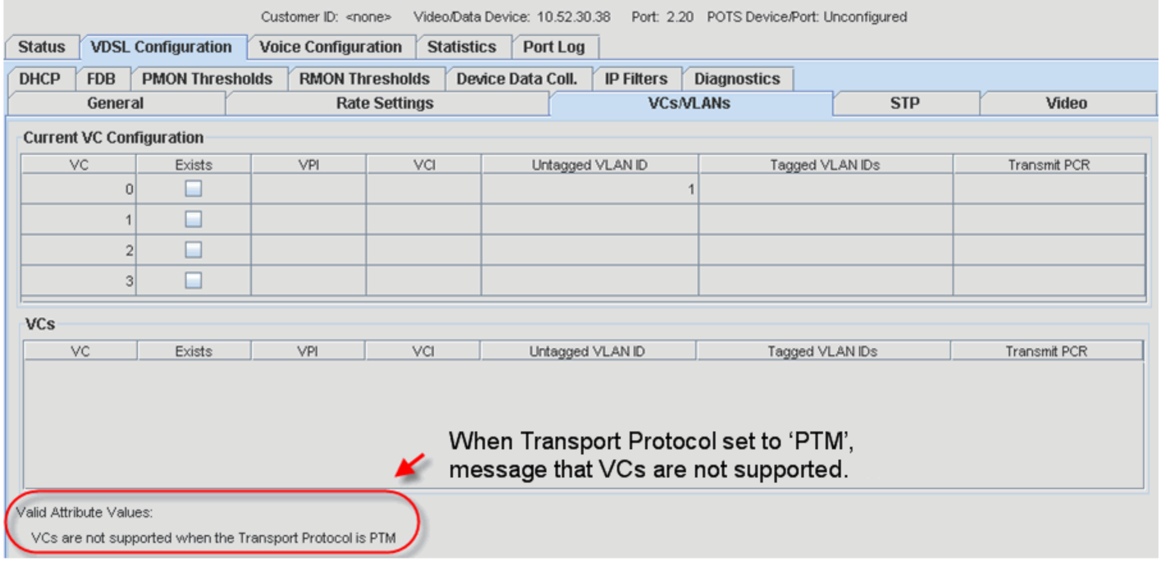
	Current Value
Admin. State/Status:	Up
Oper. State/Link State:	Down
Status:	Dependency
Connection State:	Unknown
Actual Line Std.:	Unknown
Actual DataBoost:	Unknown
Actual Line Type:	Unknown
Actual Inv G994 Vendor ID:	
Actual Inv System Vendor ID:	
Actual Inv Version Number:	
Actual Inv Serial Number:	
Actual Self Test Result:	
Actual Power Mgmt State:	Unknown
Actual Power Mgmt Status:	Unknown
Interface Profile Name:	None

	Current Value	New Value
Profile :	None	
Description (Customer ID):		
VDSL Mode:	ADSL2+	VDSL2
VDSL Line Type:	Interleave	
VDSL DataBoost:	Off	
Line Quality Monitor:	Medium	
Band Plan Profile:	8A	
		PTM
Power Mgmt Reentry Delay (1..255 secs):	180	

Message

VCs are not supported when the Transport Protocol is set to PTM. Any existing VCs will be removed from the port.

FIGURE 9-14 Message if Change Mode to PTM



Customer ID: <none> Video/Data Device: 10.52.30.38 Port: 2.20 POTS Device/Port: Unconfigured

Current VC Configuration

VC	Exists	VPI	VCI	Untagged VLAN ID	Tagged VLAN IDs	Transmit PCR
0	□			1		
1	□					
2	□					
3	□					

VCs

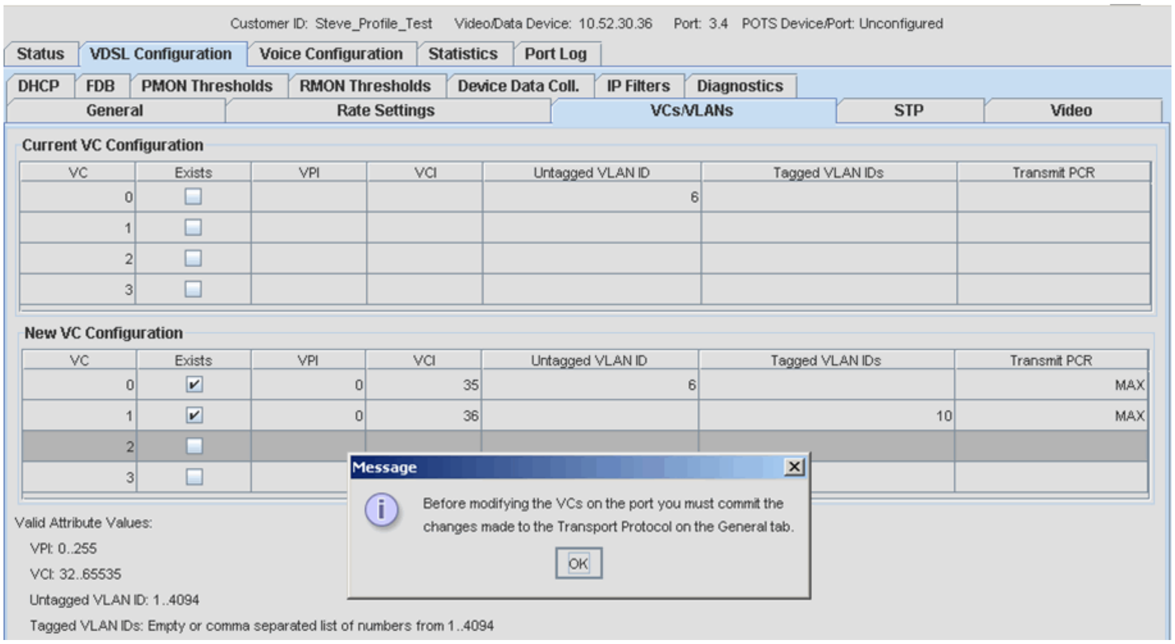
VC	Exists	VPI	VCI	Untagged VLAN ID	Tagged VLAN IDs	Transmit PCR

When Transport Protocol set to 'PTM', message that VCs are not supported.

Valid Attribute Values:
VCs are not supported when the Transport Protocol is PTM

FIGURE 9-15 VCs/VLAN tab when in PTM Mode

Changes to the View/Modify tabs are done on a per tab basis. As an example, if someone makes changes to the General tab and then makes changes to the VCs/VLANs tab, pressing the "Modify" button will only pick up the current tabs changes. Because of this, an administrator can change the Transport to "ATM" (from "PTM") and then make changes to the VCs/VLANs table. If they then attempt to save the changes to the VCs/VLANs table by selecting the "Modify" button, the data would not be valid if sent to the port because it would still be configured as "PTM". In this situation, a dialog box is opened to indicate that the changes made to the General tab must be saved prior to saving the changes on the VCs/VLANs tab. Refer to the following figure.



Customer ID: Steve_Profile_Test Video/Data Device: 10.52.30.36 Port: 3.4 POTS Device/Port: Unconfigured

Current VC Configuration

VC	Exists	VPI	VCI	Untagged VLAN ID	Tagged VLAN IDs	Transmit PCR
0	☐			6		
1	☐					
2	☐					
3	☐					

New VC Configuration

VC	Exists	VPI	VCI	Untagged VLAN ID	Tagged VLAN IDs	Transmit PCR
0	☑	0	35	6		MAX
1	☑	0	36		10	MAX
2	☐					
3	☐					

Message

Before modifying the VCs on the port you must commit the changes made to the Transport Protocol on the General tab.

Valid Attribute Values:
VPI: 0..255
VCI: 32..65535
Untagged VLAN ID: 1..4094
Tagged VLAN IDs: Empty or comma separated list of numbers from 1..4094

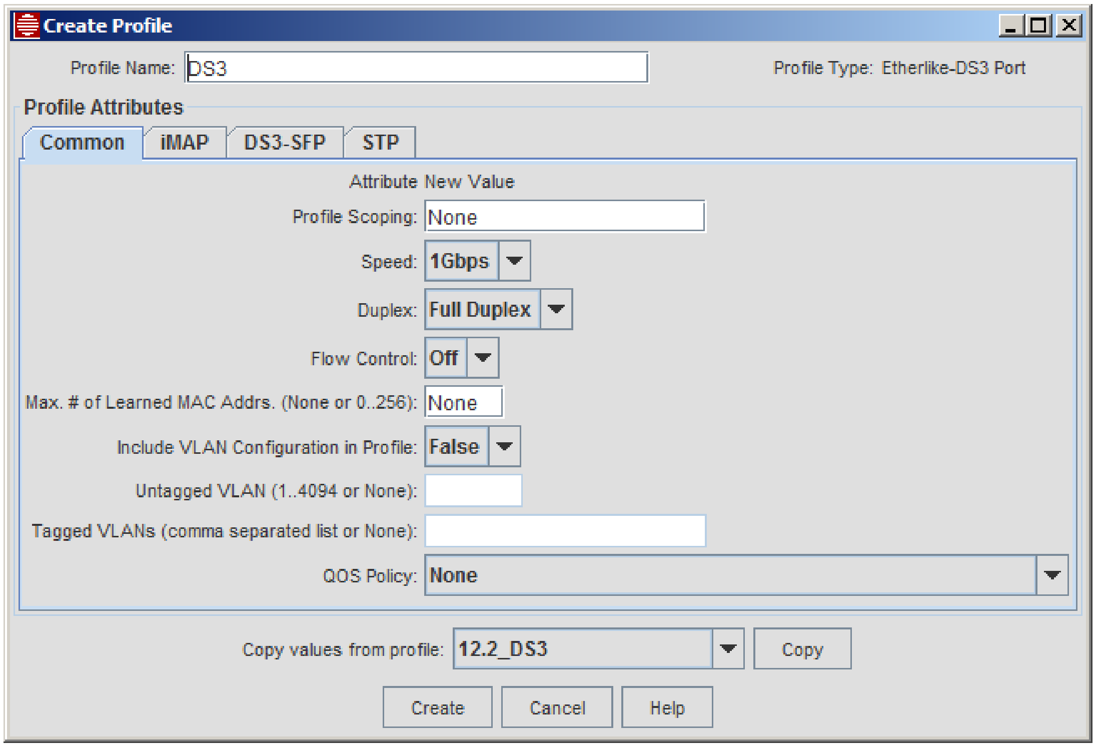
FIGURE 9-16 Message to Save Protocol Change before changing VC Configuration

9.15 DS3-SFP Support

To provide DS3 support, the 9000 iMAP devices (except the 9100) add support for a DS3-SFP. (This is currently the MiRICi-T3, which integrates a complete DS3 interface and a Gigabit Ethernet interworking function into the form factor of a standard SFP optics device.)

To provision a GE3/GE8 port that includes DS3-SFP, create an Etherlike DS3 profile:

1. From the **Network Objects** panel, select **Network Service Data > Profiles** to open the **Profiles** screen.
2. In the menu bar, go to **Network Services > Profile > Port Profiles > Create Etherlike DS3 Profile**. The Create Profile box appears.



Create Profile

Profile Name: DS3

Profile Type: Etherlike-DS3 Port

Profile Attributes

Attribute New Value

Profile Scoping: None

Speed: 1Gbps

Duplex: Full Duplex

Flow Control: Off

Max. # of Learned MAC Addrs. (None or 0..256): None

Include VLAN Configuration in Profile: False

Untagged VLAN (1..4094 or None):

Tagged VLANs (comma separated list or None):

QOS Policy: None

Copy values from profile: 12.2_DS3

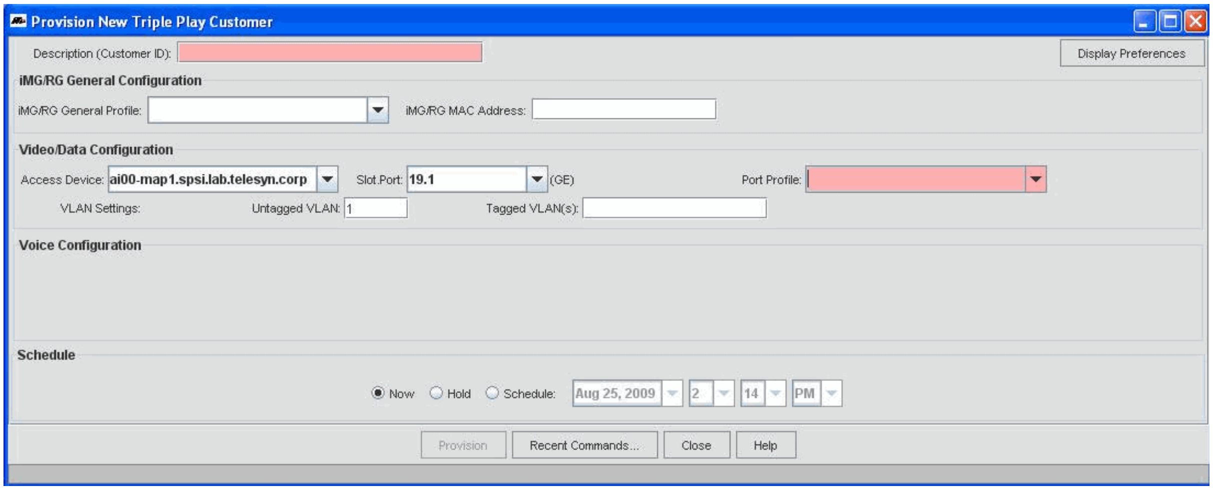
FIGURE 9-17 Create Profile - Etherlike DS3

The profile is used to provision both the Ethernet and DS3 interfaces and has four tabs:

- Common - This is similar to the Common tab for the Etherlike port Profile, except that the Speed must be set to 1Gbps and Duplex must be Full Duplex. (Auto Negotiation is not supported).
- iMAP - This tab is similar to Etherlike Port profile. The default Direction for this configuration is set to Network, which disables the DHCP parameters.
- DS3-SFP - This is specifically for the GE port that will include the DS3-SFP, and these parameters must be coordinated with those at the other end.
- STP - This is similar to the Etherlike Port profile.

Caution: To ensure that the user does not set an egress rate that exceeds the capacity of the DS3 (45Mbps), you must, in the iMAP tab, provision an Egress Rate Limiter that does not exceed the 45Mbps rate. If it is not set, you receive a warning about this and that currently no Egress Rate Limiter is set. If you do type in an Egress Rate Limiter, you receive the same warning and that the Rate Limiter typed in must not exceed 45Mbps.

To provision the DS3-SFP, select an unused Ethernet port (GE or GE8) and select Provision New Customer/Port. The only fields that need to be filled in are the Customer ID and Port Profile, as shown in the following figure.



Provision New Triple Play Customer

Description (Customer ID):

iMG/RG General Configuration

iMG/RG General Profile:

iMG/RG MAC Address:

Video/Data Configuration

Access Device: ai00-map1.spsi.lab.telesyn.corp

Slot.Port: 19.1 (GE)

Port Profile:

VLAN Settings: Untagged VLAN: 1 Tagged VLAN(s):

Voice Configuration

Schedule

● Now ○ Hold ○ Schedule: Aug 25, 2009 2 14 PM

FIGURE 9-18 Provision Etherlike Port for DS3-SFP

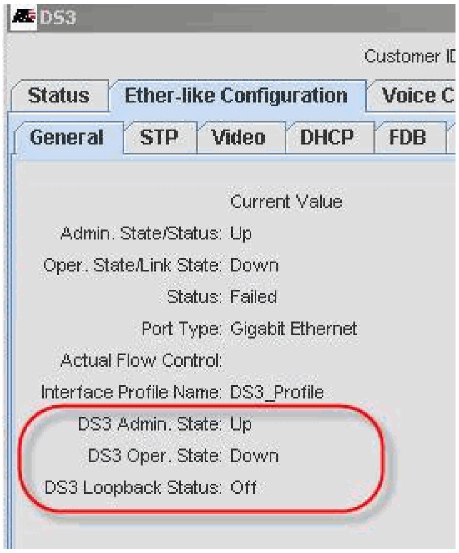
After the fields are filled in and **Provision** is selected, the status of the port changes, with the Customer ID included and the Status being:

- Down if the SFP has not been inserted, or the Ethernet or DS3 interface has failed.
- Up if an SFP has been inserted and both interfaces are operationally up.

Note: For traffic to flow, both the DS3 and GE interfaces must be operationally up, and any condition that causes one to go operationally down (such as an alarm or being administratively disabled) will cause the other to go operationally down with a failing condition and alarm.

Once the port is provisioned, you can review the in the Service Management Details for the port. This is similar to other Ethernet ports except for the following:

- General - The state of the DS3 link. Note that the relationship between the DS3 and the associated GE interface is associative rather than parent/child. Refer to the following figure.



DS3

Customer ID

Current Value

Admin. State/Status: Up

Oper. State/Link State: Down

Status: Failed

Port Type: Gigabit Ethernet

Actual Flow Control:

Interface Profile Name: DS3_Profile

DS3 Admin. State: Up

DS3 Oper. State: Down

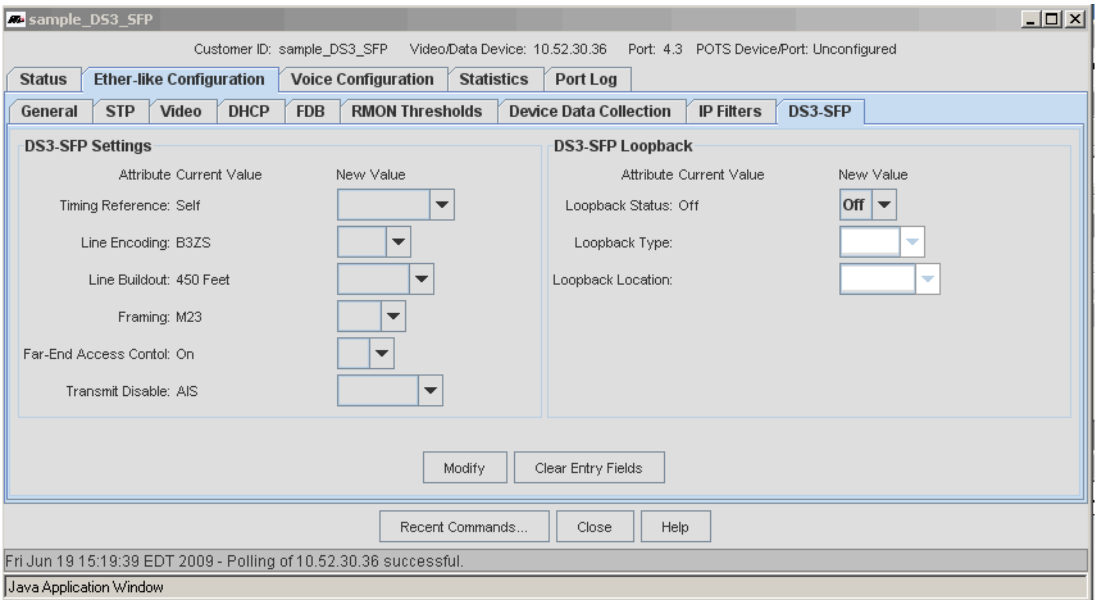
DS3 Loopback Status: Off

FIGURE 9-19 DS3 - EtherLike Configuration, General Tab

- DS3-SFP - This is under the Ether-like Configuration tab, and not only the DS3-SFP settings, but the setting of the Loopback Status. If set to On, the Loopback Type and Location are activated and can be set.

Note: The port must be operationally down to set a loopback.

Refer to the following figure.



Customer ID: sample_DS3_SFP Video/Data Device: 10.52.30.36 Port: 4.3 POTS Device/Port: Unconfigured

DS3-SFP Settings

Attribute	Current Value	New Value
Timing Reference:	Self	
Line Encoding:	B3ZS	
Line Buildout:	450 Feet	
Framing:	M23	
Far-End Access Contol:	On	
Transmit Disable:	AIS	

DS3-SFP Loopback

Attribute	Current Value	New Value
Loopback Status:	Off	Off
Loopback Type:		
Loopback Location:		

Fri Jun 19 15:19:39 EDT 2009 - Polling of 10.52.30.36 successful.

FIGURE 9-20 DS3-SFP tab

10. Quality of Service (QoS)

Configuring QoS capabilities on the various iMAP device types is fairly detailed and complex. Since the same QoS configuration is often applied across multiple devices, it is convenient for the network manager to define **QoS Policies** (configuration information) in the NMS and then separately deploy the policies to a specific set of devices and their ports.

QoS configuration interacts with the profile management, particularly with respect to activation of QoS Policies. The Profile Management Feature manages Port Profiles which include references to the QoS Policies that are to be associated with a device port.

Note: There are also Device Policies that allow for the setting of switch-wide QoS parameters to a set of devices.

The following table lists the major areas for configuring traffic management and should help the user find the appropriate information or task.

TABLE 10-1 **Task List for Traffic Management**

Task	Screen / Form Name (if Applicable)	Section
Overview of Traffic Management Concepts		("Overview of Traffic Attributes" on page 228)
QoS Traffic Flows	QoS Policy Flow Dialog	("QoS Flows" on page 229)
QoS Priority Action	QoS Priority Action Form	("QoS Priority Action" on page 233)
QoS Traffic Action	QoS Traffic Action Form	("QoS Traffic Action Form" on page 235)
QoS Policy Action	QoS Policy Action Form	("QoS Policy Action Form" on page 239)
QoS Policy Maintenance Window	QoS Policy Maintenance Window	("QoS Policy Maintenance Window (Defining a Policy)" on page 241)
QoS Policy Rule form	Edit QoS Policy Rule form	("QoS Policy Rule Form" on page 243)

10.1 Overview of Traffic Attributes

The following concepts are used when configuring QoS. These concepts follow the configuration screens that make up the creation of policies and are usually filled in this order.

- **Device Class** - A class (or set) of the same type of devices. Following are the device classes:
  - Rapier

- SwitchBlade
- iMAP
- AT8900
- ATRouter
- iMAP_EPON
- AlliedWare Plus

Device classes may or may not share certain QoS capabilities.

- **QoS Policy Action** - A QoS policy action is specifically for a Rapier or Switchblade device. It involves actions that apply to all flows on the port.
- **QoS Policy Flow** - A QoS flow refers to a substream of packets on a port that satisfies a set of classification conditions. For example, a stream of packets classified by the condition that their destination TCP port is 80 (i.e., TCPDPORT=80) is considered a QoS flow.
- **QoS Priority Action** - A QoS priority action prioritizes a QoS policy flow according to the 802.1 VLAN priority fields or the IP DSCP/TOS fields.
- **QoS Traffic Action** - A QoS traffic action refers to policing or conditioning of a flow, such as limiting the maximum bandwidth or guaranteeing a minimum bandwidth.
- **QoS Policy Rule** - A QoS policy rule is the association of a flow, priority action, and traffic action. To apply traffic conditioning to aggregate flows where the individual flows have different priorities, multiple flow-priority pairs can be entered with a single traffic action.

Note: The NMS will only allow traffic conditioning on multiple flows if all of the target device classes specified support this capability.

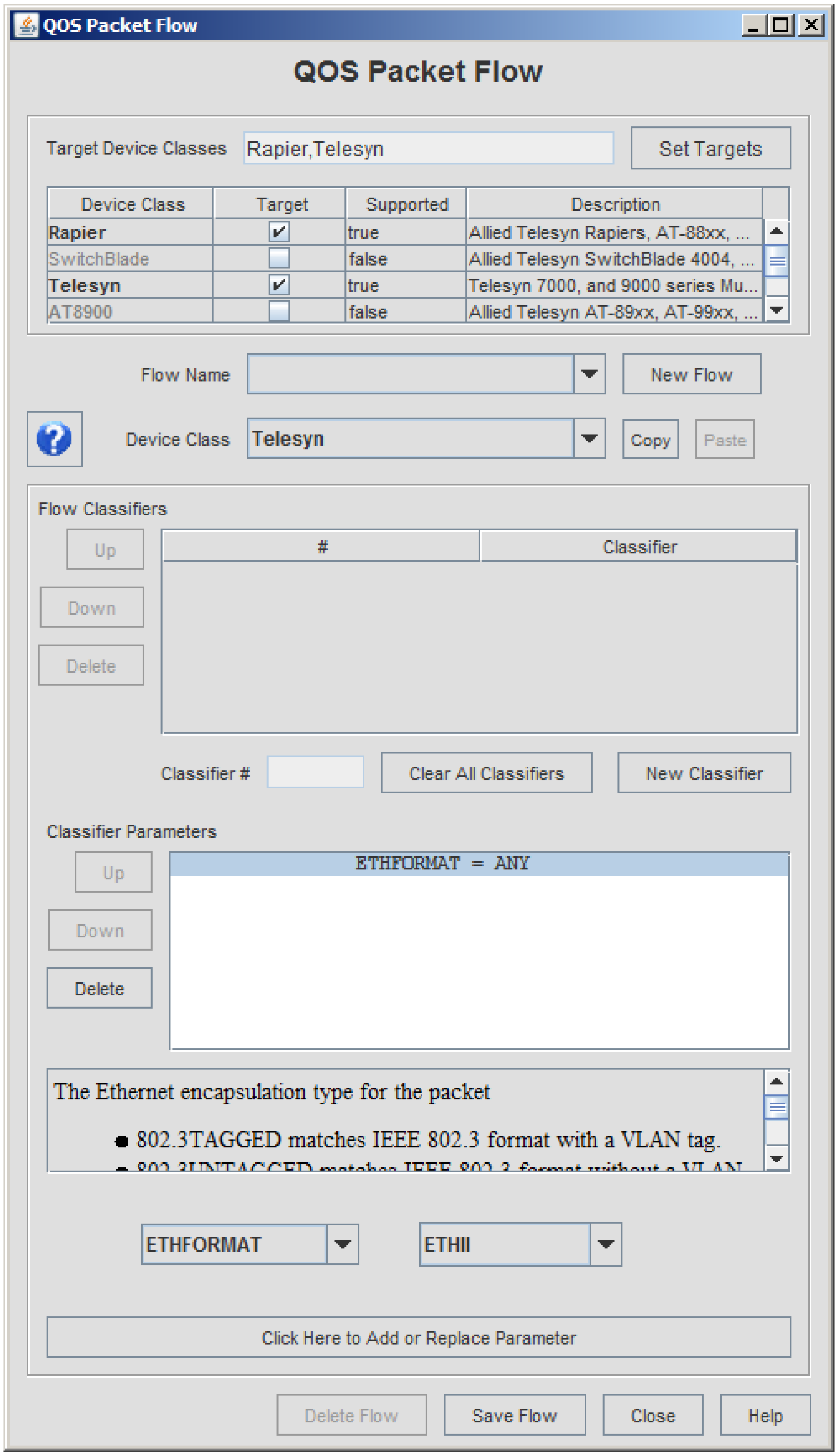
- **QoS Policy** - A QoS policy is the result of combining the QoS policy rules into a set so that, taken as a whole, it can be applied to a port or set of ports.

To create a QoS policy, you create the attributes of the policy and then associate them together to create the policy. For a detailed discussion of traffic attributes and classifier management, see the *Software Reference for iMAP Series Switches* and *Software Reference for SwitchBlade x3100 Series* user guides.

10.2 QoS Flows

To create a QoS flow:

1. In the **Network Objects** panel, go to **Network Service Data** > **QoS Policies**. This enables the **Network Services** menu item.
2. Go to **Network Services** > **QoS** > **Packet Flow**. The **QoS Packet Flow** box appears.



QOS Packet Flow

Target Device Classes: Rapier,Telesyn

Device Class	Target	Supported	Description
Rapier	☑	true	Allied Telesyn Rapiers, AT-88xx, ...
SwitchBlade	□	false	Allied Telesyn SwitchBlade 4004, ...
Telesyn	☑	true	Telesyn 7000, and 9000 series Mu...
AT8900	□	false	Allied Telesyn AT-89xx, AT-99xx, ...

Flow Name:

Device Class: Telesyn

#	Classifier

Classifier #:

ETHFORMAT = ANY

The Ethernet encapsulation type for the packet

- 802.3TAGGED matches IEEE 802.3 format with a VLAN tag.
- 802.3UNTAGGED matches IEEE 802.3 format without a VLAN

ETHFORMAT ETHII

FIGURE 10-1 QoS Policy Flow

QoS Packet Flow contains the following fields:

TABLE 10-2 QoS Packet Flow

Option	Purpose
Target Device Classes	The device classes to be included in this flow.
Set Targets	Brings up the Edit QOS Device Class List, allowing the user to select any combination of device classes to include.Press and Hold the SHift key to select more than one device class. Targets can also be added/removed by clicking the “Target” checkbox.
Device Class table	Table of the Device Classes, Targets, and a description of the device class. Supported indicates there are no detected errors.
Flow Name	A pull-down of all existing flows.If selected, the parameters of the selected flow appear in the form.
Device Class	A pull-down of the device classes that are included in this policy. This reflects the tic boxes chosen in the Device Class table.
New Flow	Brings up the Select New Name window. The user can choose to copy the parameters from the flow currently displayed.
Copy	Saves the parameters from the current Device Class target so they can be 'pasted' to another target device class by the “translation” feature.
Paste	Translates and applies the parameters that were “copied”. If there is no translation for a parameter it will appear with square brackets around it, and be colored red. If there is similar parameter but the value cannot be translated the value will be enclosed in square brackets and the entry will again be colored red.
Flow Classifiers	A table of the current classifiers. Delete removes the selected classifier. The Up and Down buttons change the **order** of classifiers (and so the logical OR), but not the selection.
Classifier #	The number of the classifier in the list. The order determines the precedence of the rules
Clear All Classifiers	Delete all classifiers in the Flow Classifier table and return to the default classifier and value (ETHFORMAT=ANY).
New Classifier	Adds a classifier to the Flow Classifier table with the default classifier and value (ETHFORMAT=ANY). This classifier appears in the Classifier Parameter list and can be modified or replaced
Classifier Parameters	A list of the parameters for the selected classifier. If more than one parameter is listed, the Up, Down, and Delete buttons are active. The Up and Down buttons change the order of classifiers (and so the logical AND), but the order does not affect the function
Parameter pull-down and value field	A pull-down of the available parameters. As each one is selected, the associated value field appears. Values may be selected from a list of values, where each element of the list can be a Name, an IP or MAC address, an integer range, a fixed point decimal range, or hexadecimal value. One parameter TCPFLAGS is a list of named values selected with a drop-down menu. For example, selecting VID will bring up a value field with 500, a default value. The user can then overwrite this value of 500.
Click Here to Add or Replace Parameter	If the parameter is not in the Flow Classifier table, it is added to the parameter list for that classifier (and creating another AND condition). If the parameter has already been chosen, it replaces what is already there with the new value. The available Parameters and Values change as parameters are added, reflecting the interdependencies between the parameters. For example if TCPDPORT is selected, PROTOCOL is added with a value of IP and it range is restricted to only IP
Delete Flow	Deletes the flow entry for all Target Device Classes. To remove the flow for a single Device Class uncheck its “target” checkbox. When the flow is saved the entry for that Device Class will be removed from the database.

TABLE 10-2 QoS Packet Flow

Option	Purpose
Save Flow	If a new flow has been defined, an existing been has been changed, or targets have been removed, makes the changes permanent. If the parameters for some device classes are incomplete, a message box will appear with options to Fix, Skip, or Cancel. The Fix button will take you to the in error device class entry. *Note: If the flow (or action) is used by a policy that is already deployed, the Deployment Record will be marked out of sync. This takes into account what device classes actually changed.*
Close	Closes the form. If any changes have been made a Verify Close window asks to make these changes permanent.

A QoS flow requires a name and a defined set of classifier conditions that is device-specific. You can define multiple parameters within the set to create an AND condition. To add a logical OR to the flow definition, you can add another set of classifier conditions.

Table 10-3 lists the flow conditions for the various device classes, highlighting which parameters are the same, different, or the same but with slightly different parameter names. When you copy and paste flows parameters are automatically translated between devices.

TABLE 10-3 QoS Conditions for Device Classes

Function	SwitchBlade	Rapier	8900	iMAP	AlliedWare Plus
Ethernet Encapsulation	ETHFORMAT PROTOCOL	ETHFORMAT PROTOCOL	ETHFORMAT PROTOCOL	ETHFORMAT	ETHFORMAT PROTOCOL
MAC Address / VLAN	DVLAN, SVLAN MACTYPE	VLAN MACSADDR MACDADDR	VLAN MACSADDR MACDADDR MACTYPE	VLANID MACSOURCE MACDEST	-
IP Address	IPDADDR IPSADDR	IPDADDR IPSADDR	IPDADDR IPSADDR	IPDEST IPSOURCE	-
IPX	IPXDADDR IPXDSOCKET IPXSSOCKET	IPXDADDR IPXDSOCKET IPXSSOCKET IPXPACKET	IPXDADDR IPXDSOCKET IPXSSOCKET	-	
Layer 4 Protocol Address and Type	IPPROTOCOL TCPDPORT TCPSPORT UDPDPORT UDPSPORT	IPPROTOCOL TCPDPORT TCPSPORT UDPDPORT UDPSPORT TCPFLAGS	IPPROTOCOL TCPDPORT TCPSPORT UDPDPORT UDPSPORT	IPPROTOCOL TCPPORTDEST TCPPORTSOURCE UDPPORTDEST UDPPORTSOURCE TCPFLAGS	IPPROTOCOL TCPFLAGS TPID INNERTPID TCPFLAGS
IPTOS / DiffServ / VLAN Priority	IPDSCP, IPTOS	IPDSCP, IPTOS	IPDSCP, IPTOS	IPDSCP, IPTOS VLANPRIORITY	IPPRECEDENCE

TABLE 10-3 QoS Conditions for Device Classes (Continued)

Function	SwitchBlade	Rapier	8900	iMAP	AlliedWare Plus
General Pattern Match	-	MATCH1, MASK1, OFFSET1, ...		-	-
Ingress / Egress Port	-	EPORT IPORT		-	-

10.3 QoS Priority Action

To create a set of priority actions (which can be associated with a QoS Flow), one or more priority action parameters are defined and given a name.

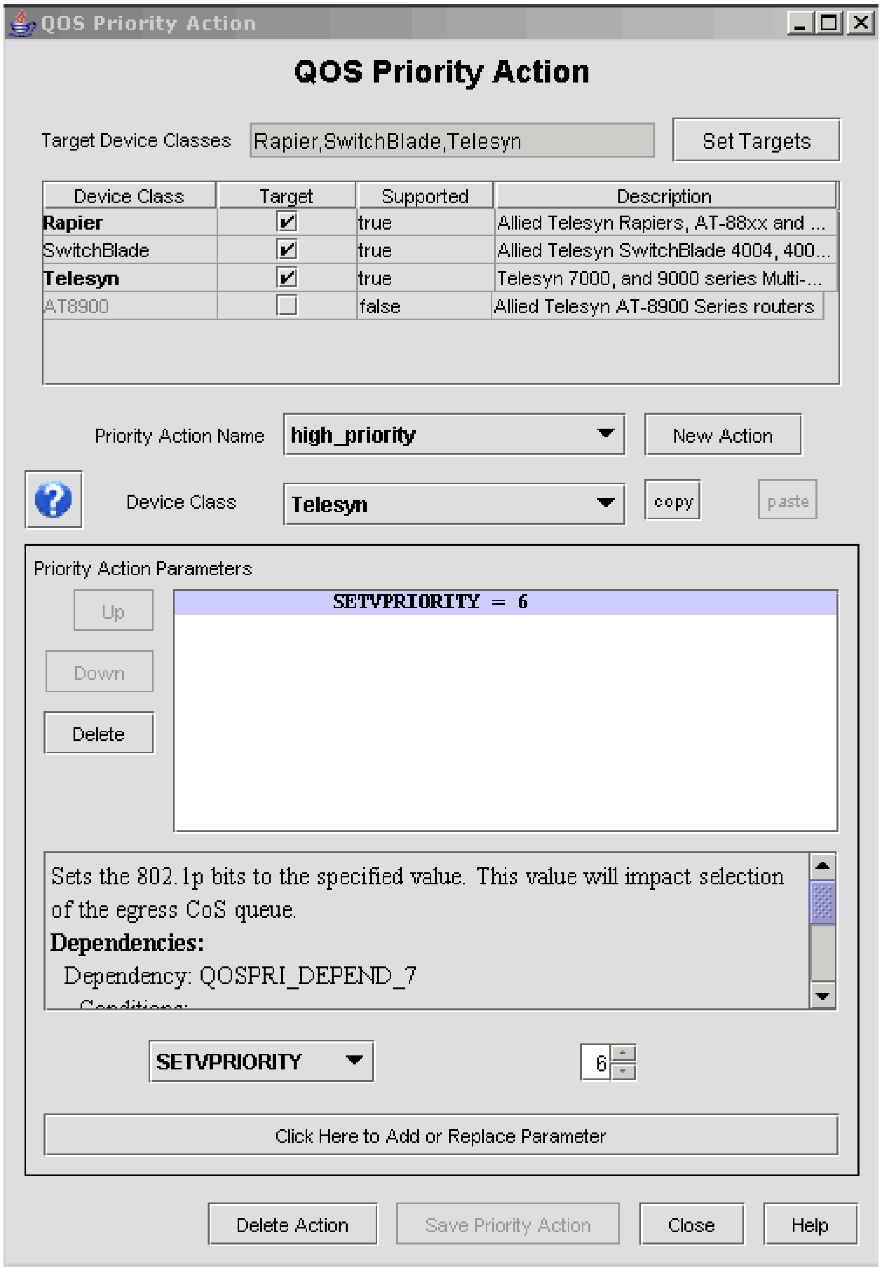
Note: These parameters can be applied to one or more device classes, as long as they all support the same parameter. If they do not, an error message appears.

Table 10-4 lists the allowable actions that can be assigned to a flow. conditions for the various device classes, and highlights which parameters are the same, different, or the same but with slightly different parameter names

TABLE 10-4 QoS Priority Actions for Device Classes

Function	SwitchBlade	Rapier	iMAP	AlliedWare Plus
Remark the DSCP value at the Ingress port	-	MARKVALUE	SETIPTOS SETIPDSCP MOVEPRIOTOTOS	-
Remark the DSCP value at Egress port	MARKVALUE	-	-	DSCP
Set queue priority at Ingress port / Remark the VLAN p-bits option	-	PRIORITY REMARKPRIORITY	SETVLANPRIORITY MOVETOSTORPIO	COS
Set queue priority at Egress port / (no remark of the VLAN p-bits option)	PRIORITY	-	-	-
Drop / Forward traffic from flow (ingress port)	-	-	DROP, FORWARD	-
Traffic Statistics (Ingress port)	-	-	COUNT	-
Congestion Control (Egress Port)	RED	-	-	-

To access the Priority Action Form, select *QoS -> Action -> Priority Action*. Figure 10-2 shows an example QoS Priority Action Form. Table 10-5 describes the fields



QOS Priority Action

Target Device Classes: Rapier,SwitchBlade,Telesyn

Device Class	Target	Supported	Description
Rapier	☑	true	Allied Telesyn Rapiers, AT-88xx and ...
SwitchBlade	☑	true	Allied Telesyn SwitchBlade 4004, 400...
Telesyn	☑	true	Telesyn 7000, and 9000 series Multi-...
AT8900	☐	false	Allied Telesyn AT-8900 Series routers

Priority Action Name: **high_priority**

Device Class: **Telesyn**

Priority Action Parameters

```
SETVPRIORITY = 6
```

Sets the 802.1p bits to the specified value. This value will impact selection of the egress CoS queue.

Dependencies:

Dependency: QOSPRI_DEPEND_7

Conditions:

SETVPRIORITY: 6

FIGURE 10-2 QoS Priority Action Form - iMAP Device

.

TABLE 10-5 Options for the QoS Priority Action Form

Option	Purpose
Target Device Classes	The device classes to be included in this Flow.
Set Targets	Brings up the Edit QOS Device Class List, allowing the user to select any combination of device classes to include.Press and Hold the SHift key to select more than one device class. Targets can also be added/removed by clicking the “Target” checkbox.

TABLE 10-5 Options for the QoS Priority Action Form

Option	Purpose
Device Class table	Table of the Device Classes, Targets, and a description of the device class. Supported indicates there are no detected errors.
Priority Action Name	A pull-down of all existing actions. If selected, the parameters of the selected action appear in the form.
Device Class	A pull-down of the device classes that are included in this policy. This reflects the tic boxes chosen in the Device Class table.
New Action	Brings up the Select New Name window. The user can choose to copy the parameters from the action currently displayed.
Copy	Saves the parameters from the current Device Class target so they can be 'pasted' to another target device class by the “translation” feature.
Paste	Translates and applies the parameters that were “copied”. If there is no translation for a parameter it will appear with square brackets around it, and be colored red. If there is similar parameter but the value cannot be translated the value will be enclosed in square brackets and the entry will again be colored red.
Priority Action Parameters	A list of the parameters for the selected action. If more than one parameter is listed, the Up, Down, and Delete buttons are active.
Parameter Description	For the parameter chosen in the Priority Action Parameters list, a description of what the parameter is and what it does.
Parameter pull-down and value field	A pull-down of the available parameters. As each one is selected, the associated value field appears. For example, selecting SETVPRIORITY will bring up a value field with 0, a default value. The user can then overwrite this value of 1 to 7. For other parameters, such as MARKVALUE, the value field is another pull-down of the available values.
Click Here to Add or Replace Parameter	If the parameter is not in the Priority Action list, it is added. If the parameter has already been chosen, it replaces what is already there with the new value. The available Parameters and Values change as parameters are added, reflecting the interdependencies between the parameter
Delete Action	Deletes the Priority Action entry for all Target Device Classes. To remove the action for a single Device Class uncheck its “target” checkbox. When the action is saved the entry for that Device Class will be removed from the database.
Save Priority Action	If a new action has been defined, an existing action has been changed, or targets have been removed, makes the changes permanent. If the parameters for some device classes are incomplete, a message box will appear with options to Fix, Skip, or Cancel. The Fix button will take you to the in error device class entry. *Note: If the Action is used by a policy that is already deployed, the Deployment Record will be marked out of sync. (Takes into account what device Classes actually changed)*
Close	Closes the form. If any changes have been made a Verify Close window asks to make these changes permanent.

10.4 QoS Traffic Action Form

To define a traffic action (a condition or set of conditions that can be used on a traffic flow), one or more traffic action parameters are defined and given a name.

Note: These parameters can be applied to one or more device classes, as long as they all support the same parameter. If they do not, an error message appears.

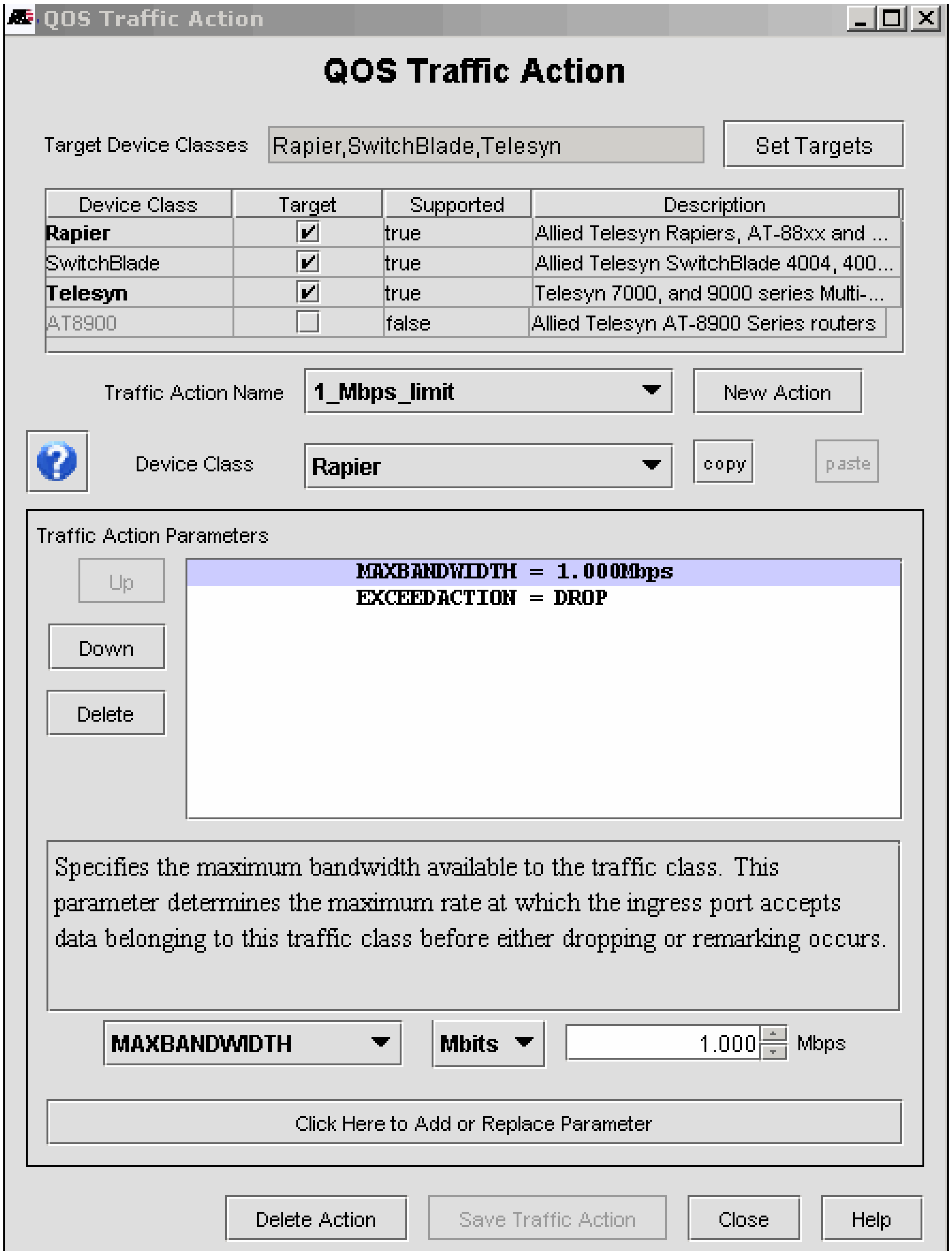
Table 10-6 lists the allowable actions that can be assigned to a traffic action for the various device classes, and highlights which parameters are the same, different, for the same but with slightly different parameter names

TABLE 10-6 QoS Traffic Actions for Device Classes

Function	SwitchBlade	Rapier	iMAP	AlliedWare Plus
Ingress Traffic Policing - handling non-conforming traffic	-	MAXBANDWIDTH EXCEEDACTION EXCEEDREMARKVALUE	RATE BUFFERSIZE NCDROP NCFORWARD NCREMARKDSCP NCCOUNT	METER PBS
Egress Traffic Limiting / Scheduling	MAXBANDWIDTH MINBANDWIDTH FAIRHASHEDFLOWS WEIGHT STATS	-	RATE BUFFERSIZE	CBS CIR EBS EIR PBS
Congestion Control (Egress Queueing)	RED	-	-	STORMACTION STORMDOWNTIME STORMPROTECTION STORMRATE STORMWINDOW

To access the Traffic Action Form, select *QoS -> Actions -> Traffic Actions*. Figure 10-3 shows an example QoS Policy Rule Form. Table 10-7 describes the fields.

Note: For the iMAP_EPON interface, refer to "Example of an EPON/ONU Interface Policy" on page 253



QOS Traffic Action

Target Device Classes: Rapier,SwitchBlade,Telesyn

Device Class	Target	Supported	Description
Rapier	☑	true	Allied Telesyn Rapiers, AT-88xx and ...
SwitchBlade	☑	true	Allied Telesyn SwitchBlade 4004, 400...
Telesyn	☑	true	Telesyn 7000, and 9000 series Multi-...
AT8900	☐	false	Allied Telesyn AT-8900 Series routers

Traffic Action Name: **1_Mbps_limit**

Device Class: **Rapier**

Traffic Action Parameters

```
MAXBANDWIDTH = 1.000Mbps
EXCEEDACTION = DROP
```

Specifies the maximum bandwidth available to the traffic class. This parameter determines the maximum rate at which the ingress port accepts data belonging to this traffic class before either dropping or remarking occurs.

MAXBANDWIDTH **Mbits** 1.000 Mbps

FIGURE 10-3 QoS Traffic Action Form - Rapier

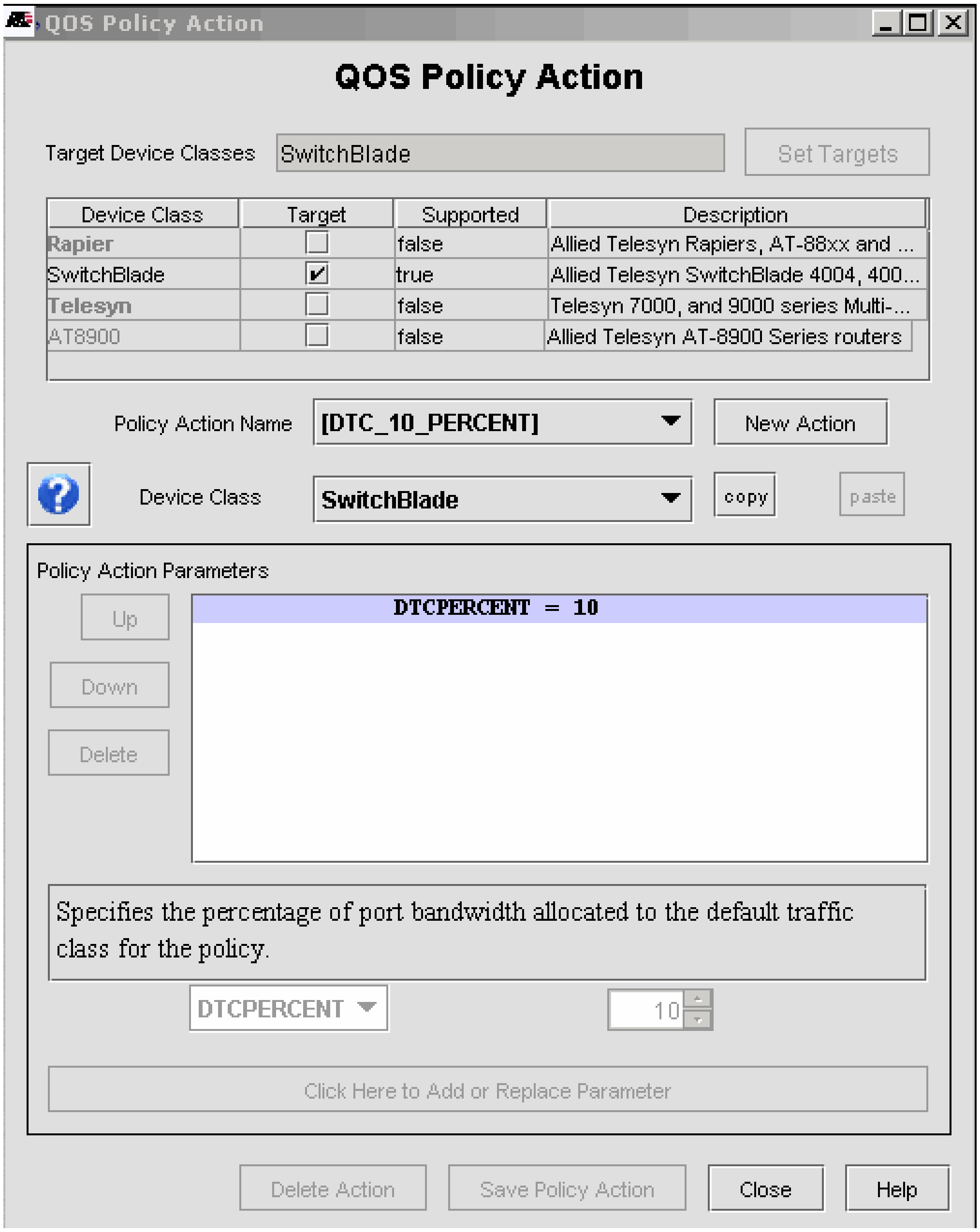
TABLE 10-7 Options for the QoS Traffic Action Form

Option	Purpose
Target Device Classes	The device classes to be included in this Traffic Action.
Set Targets	Brings up the Edit QOS Device Class List, allowing the user to select any combination of device classes to include.Press and Hold the SHift key to select more than one device class. Targets can also be added/removed by clicking the “Target” checkbox.
Device Class table	Table of the Device Classes, Targets, whether the parameters chosen are supported by the device class, and a description of the device class.
Traffic Action Name	A pull-down of all existing Traffic Actions. If selected, the parameters of the selected action appear in the form.
Device Class	A pull-down of the device classes that are included in this policy. This reflects the tic boxes chosen in the Device Class table.
New Action	Brings up the Select New Name window. The user can choose to copy the parameters from the action currently displayed.
Copy	Saves the parameters from the current Device Class target so they can be 'pasted' to another target device class by the “translation” feature.
Paste	Translates and applies the parameters that were “copied”. If there is no translation for a parameter it will appear with square brackets around it, and be colored red. If there is similar parameter but the value cannot be translated the value will be enclosed in square brackets and the entry will again be colored red.
Traffic Action Parameters	A list of the parameters for the selected action. If more than one parameter is listed, the Up, Down, and Delete buttons are active.
Parameter Description	For the parameter chosen in the Traffic Action Parameters list, a description of what the parameter is and what it does.
Parameter pull-down and value field	A pull-down of the available parameters. As each one is selected, the associated value field appears. For example, selecting RATE will bring up a value field with 1, a default value. The user can then overwrite this value. For other parameters, such as BURSTSIZE, the value field is another pull-down of the available values.
Click Here to Add or Replace Parameter	If the parameter is not in the Traffic Action Parameters list, it is added. If the parameter has already been chosen, it replaces what is already there with the new value. The available Parameters and Values change as parameters are added, reflecting the interdependencies between the parameter
Delete Action	Deletes the entire Priority Action and its associated parameters.
Save Traffic Action	If a new action has been defined, an existing action has been changed, or targets have been removed, makes the changes permanent. If the parameters for some device classes are incomplete, a message box will appear with options to Fix, Skip, or Cancel. The Fix button will take you to the in error device class entry. *Note: If Action is used by a policy that is already deployed, the Deployment Record will be marked out of sync. (Takes into account what device Classes actually changed)*
Close	Closes the form. If any changes have been made a Verify Close window asks to make these changes permanent.

10.5 QoS Policy Action Form

The device classes may also have action parameters at the policy/port level. Figure 10-4 shows an example QoS Policy Rule Form. Table 10-8 describes the fields.

Note: A policy action can be created that supports an iMAP device with a "None" option.



QOS Policy Action

Target Device Classes: SwitchBlade

Device Class	Target	Supported	Description
Rapier	□	false	Allied Telesyn Rapiers, AT-88xx and ...
SwitchBlade	☑	true	Allied Telesyn SwitchBlade 4004, 400...
Telesyn	□	false	Telesyn 7000, and 9000 series Multi-...
AT8900	□	false	Allied Telesyn AT-8900 Series routers

Policy Action Name: [DTC_10_PERCENT]

Device Class: SwitchBlade

Policy Action Parameters

DTCPERCENT = 10

Specifies the percentage of port bandwidth allocated to the default traffic class for the policy.

DTCPERCENT 10

FIGURE 10-4 QoS Policy Action Form

TABLE 10-8 Options for the QoS Policy Action Form

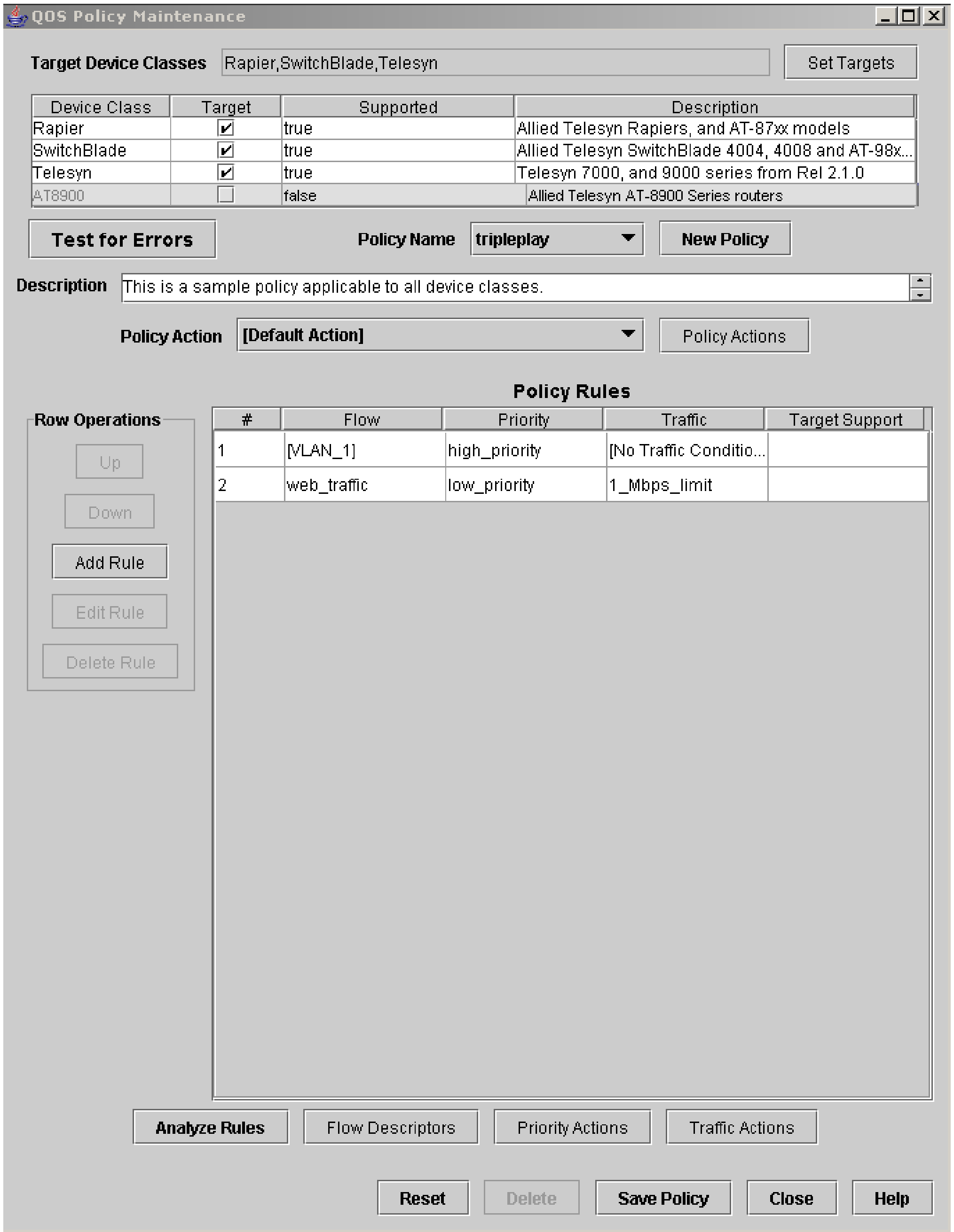
Option	Purpose
Target Device Classes	The device classes to be included in this Flow.
Set Targets	Brings up the Edit QOS Device Class List, allowing the user to select any combination of device classes to include.Press and Hold the Shift key to select more than one device class. Targets can also be added/removed by clicking the “Target” checkbox.
Device Class table	Table of the Device Classes, Targets, and a description of the device class. Supported indicates there are no detected errors.
Policy Action Name	A pull-down of all existing Policy Actions. If selected, the parameters of the selected action appear in the form.
Device Class	A pull-down of the device classes that are included in this policy action. This reflects the tic boxes chosen in the Device Class table.
New Action	Brings up the Select New Name window. The user can choose to copy the parameters from the flow currently displayed.
Copy	Saves the parameters from the current Device Class target so they can be 'pasted' to another target device class by the “translation” feature.
Paste	Translates and applies the parameters that were “copied”. If there is no translation for a parameter it will appear with square brackets around it, and be colored red. If there is similar parameter but the value cannot be translated the value will be enclosed in square brackets and the entry will again be colored red.
Policy Action Parameters	A list of the parameters for the selected action. If more than one parameter is listed, the Up, Down, and Delete buttons are active.
Parameter Description	For the parameter chosen in the Policy Action Parameters list, a description of what the parameter is and what it does.
Parameter pull-down and value field	A pull-down of the available parameters. As each one is selected, the associated value field appears.
Click Here to Add or Replace Parameter	If the parameter is not in the Policy Action Parameters list, it is added. If the parameter has already been chosen, it replaces what is already there with the new value. The available Parameters and Values change as parameters are added, reflecting the interdependencies between the parameter
Delete Action	Deletes the entire Policy Action and its associated parameters.
Save Policy Action	If a new Policy Action has been defined, an existing Policy Action has been changed, or targets have been removed, makes the changes permanent. If the parameters for some device classes are incomplete, a message box will appear with options to Fix, Skip, or Cancel. The Fix button will take you to the in error device class entry. *Note: If the Action is used by a policy that is already deployed, the Deployment Record will be marked out of sync. (Takes into account what device Classes actually changed)*
Close	Closes the form. If any changes have been made a Verify Close window asks to make these changes permanent.

10.6 QoS Policy Maintenance Window (Defining a Policy)

Once all the attributes for a QoS policy have been created, they are associated to create or define a policy which has a unique name.

Note: *The names for a Policy can be up to 15 characters and should be lower case. Moreover, underscores and spaces are not allowed.*

Figure 10-5 shows the QoS Policy Maintenance window.Table 10-9 explains the options.



Target Device Classes: Rapier,SwitchBlade,Telesyn

Device Class	Target	Supported	Description
Rapier	☑	true	Allied Telesyn Rapiers, and AT-87xx models
SwitchBlade	☑	true	Allied Telesyn SwitchBlade 4004, 4008 and AT-98x...
Telesyn	☑	true	Telesyn 7000, and 9000 series from Rel 2.1.0
AT8900	□	false	Allied Telesyn AT-8900 Series routers

Policy Name: tripleplay

Description: This is a sample policy applicable to all device classes.

Policy Action: [Default Action]

Policy Rules

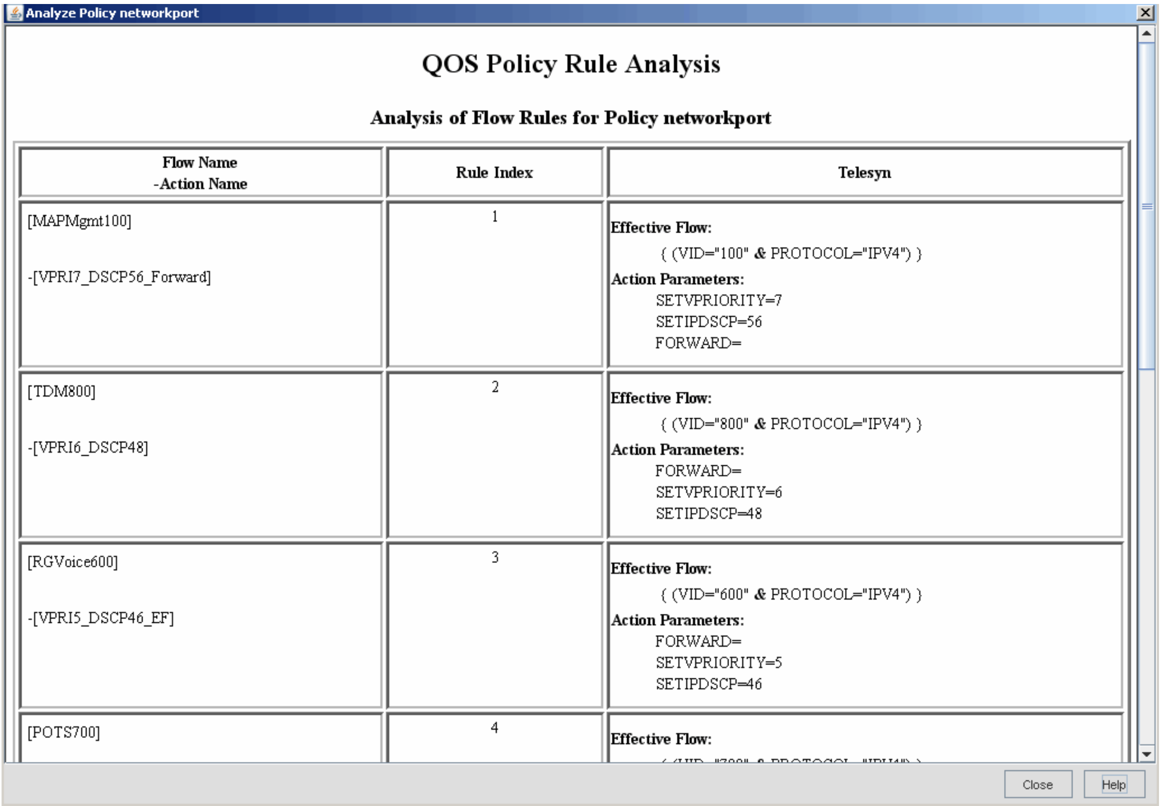
#	Flow	Priority	Traffic	Target Support
1	[VLAN_1]	high_priority	[No Traffic Conditio...	
2	web_traffic	low_priority	1_Mbps_limit	

FIGURE 10-5 QoS Policy Maintenance Window

TABLE 10-9 Options for the QoS Policy Maintenance Window

Option	Purpose
Target Device Classes	The device classes to be included in this Policy.
Set Targets	Brings up the Edit QOS Device Class List, allowing the user to select any combination of device classes to include.Press and Hold the SHift key to select more than one device class. Note that if a device class is chosen that does not support the existing rules in a Policy, an error message appears and the device class cannot be added.
Policy Name	A unique name to identify the policy. Refer to the Note above.
New Policy	Brings up a window to enter a new unique name. If this is accessed from an existing Policy, there is the option to copy the attributes from the existing policy to the new Policy.
Description	A way to provide more detail.
Policy Action	This is available for Rapier and Switchblade device classes only, and lists those that have been created.
Policy Rules table	The Policy Rules associated with the Policy. There are five columns: # - The number of the Policy Rule. Click on this to Edit, Delete, or move rules up/down. Flow - The current policy flow, which can be changed by selecting the cell. Priority - The Priority Action, which can be changed by selecting the cell. Traffic - The Traffic Action, which can be changed by selecting the cell. Target Support Flows, Priority Actions, and Traffic Actions for single flow rules can be edited directly in the table, Multi-flow rules can only be edited with the Rule Form
Analyze Rules	Goes through the defined flows and actions and applies a logic tree for the device types selected so that conflicts from a previous flow are highlighted.
Flow Descriptions	Brings up the Policy Flow Form for the selected Flow. Note that this is the standard Policy Flow Form, and so other Flows can be modified and new Flows can be created.
Priority Actions	Brings up the Priority Action Form for the selected Action. Note that this is the standard Priority Action Form, and so other Actions can be modified and new Actions can be created.
Traffic Actions	Brings up the Traffic Action Form for the selected Action. Note that this is the standard Traffic Action Form, and so other Actions can be modified and new Actions can be created.
Reset	Undo any changes that have been made by rereading the Policy from the database.
Delete	Delete the Policy and all its attributes. If the Policy has been applied to any port, an error message appears and the policy cannot be deleted.
Save Policy	Makes permanent all the changes that have been made. If the policy has already been deployed as part of Profile Management, the associated ports in the Ports table will have their Profile names marked with a “*” to indicate they are currently out-of-sync with the modified policy. To redeploy these changes, redeploy the profile as described in "Redeploying a Profile" on page 213.

The **Analyze Rules** button follows a logic tree to highlight potential conflicts between the flows and actions for the device types. The following figure is an example.



QOS Policy Rule Analysis

Analysis of Flow Rules for Policy networkport

Flow Name -Action Name	Rule Index	Telesyn

[MAPMgmt100]
-[VPRI7_DSCP56_Forward]
	1	**Effective Flow:**
		{ (VID="100" & PROTOCOL="IPV4") }
		Action Parameters:
		SETVPRIORITY=7
		SETIPDSCP=56
		FORWARD=

[TDM800]
-[VPRI6_DSCP48]
	2	**Effective Flow:**
		{ (VID="800" & PROTOCOL="IPV4") }
		Action Parameters:
		FORWARD=
		SETVPRIORITY=6
		SETIPDSCP=48

[RGVoice600]
-[VPRI5_DSCP46_EF]
	3	**Effective Flow:**
		{ (VID="600" & PROTOCOL="IPV4") }
		Action Parameters:
		FORWARD=
		SETVPRIORITY=5
		SETIPDSCP=46

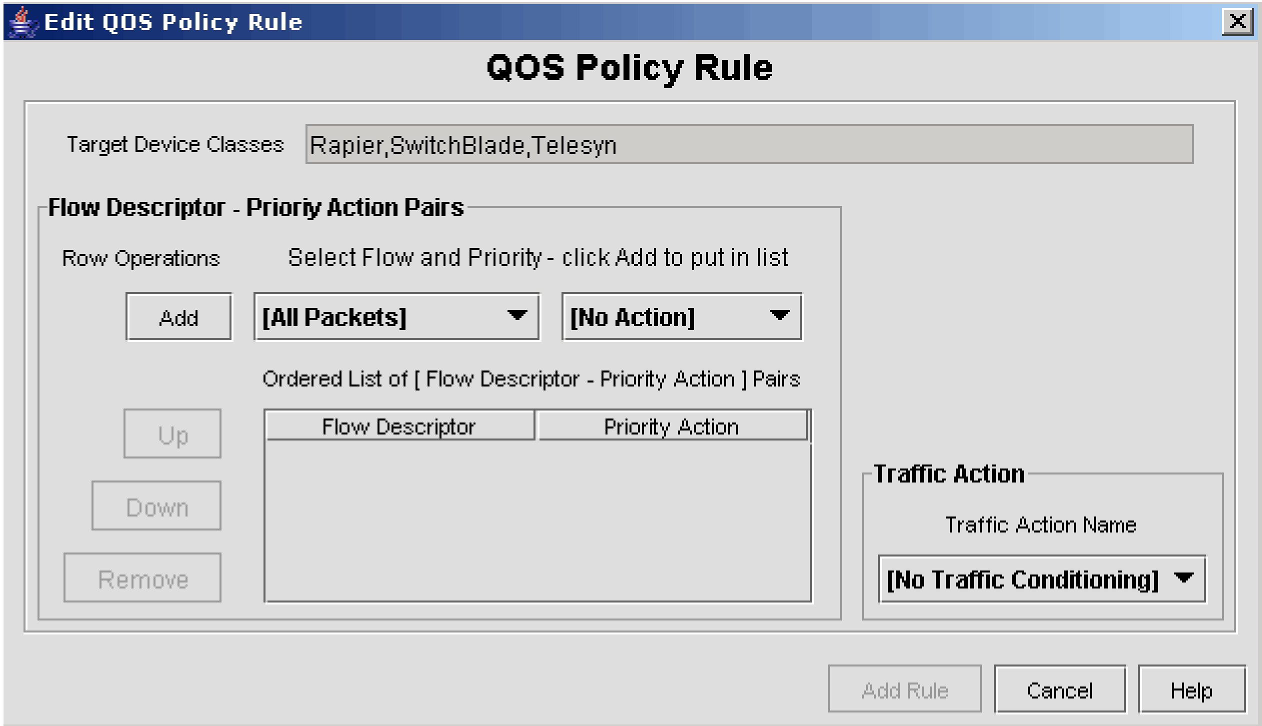
[POTS700]	4	**Effective Flow:**

FIGURE 10-6 Analyze Rules Window

10.7 QoS Policy Rule Form

To associate a flow, a priority action, and a traffic action the QoS Policy Rule Form is used. This form is accessed on the QoS Policy Maintenance Form by clicking on the **Add Rule** button.

Figure 10-7 shows an example QoS Policy Rule Form. Table 10-7 describes the fields.


Edit QOS Policy Rule
QOS Policy Rule
Flow Descriptor - Prioriy Action Pairs
Row Operations
Select Flow and Priority - click Add to put in list
Add
Up
Down
Remove
Ordered List of [Flow Descriptor - Priority Action] Pairs
Flow Descriptor
Priority Action
Traffic Action
Add Rule
Cancel
Help

Target Device Classes: Rapier,SwitchBlade,Telesyn

[All Packets]

[No Action]

Traffic Action Name: [No Traffic Conditioning]

FIGURE 10-7 QoS Policy Rule Form

TABLE 10-10 Options for the QoS Policy Rule Form

Option	Purpose
Target Device Classes	The device classes that are included in this policy. This value is read-only.
Priority Action Pairs	Two pull-downs that have the available Flow Descriptions and Priority Actions. Select one from each to include in the rule. Note that each flow name can only be used once in a policy. The combo-box values for Flow Descriptor reflect this constraint.
Traffic Action	One pull-down to select the Traffic Action associated with he Flow Description/Priority Action pair.
Add	Adds the selected Flow-Descriptor pair to the Pair Table.
Add Rule	Add the rule to the Policy. The QOS Policy Maintenance form appears with the rule included.
	Up, Down, Remove, would you want these since each rule should have one of each?

Note: *In using this form, the user must be aware that it is a two-step process; the user first selects the flow and priority and clicks on Add to add them as a Priority/Action pair. The user then chooses a traffic action and selects Add Rule to actually add the rule to the policy form as a row.*

10.8 Viewing Default Flows, Priorities, Actions, and Policies

When the NMS is first installed there is a set of flows, priorities, actions, and policies (which are made up of a combination of the these flows, priorities, and actions) that are already configured. These can be immediately used and applied to the devices and ports (and included in profiles), or used as a starting point for creating new ones. (For example, an existing flow can be brought up, and a new one can be created based on its attributes.)

Note: *Names that are enclosed in square brackets, [Name], are set by Allied Telesis and cannot be changed.*

10.9 Example of an iMAP Device Class Policy

Figure 10-8 shows a sample QoS configuration for a network, and it has the following attributes:

- The types of traffic flows are associated with specific VIDs.
- The video Head End uses the VLAN ID (VID) range of 3xx; these are then divided up into regions so that certain VIDS are configured on upstream devices that connect with an iMAP product.
- The ISP Head End uses the VID range of 5xx.
- The voice over IP gateway uses the VID range of 7xx.
- The quality of service is defined entirely through priority queueing, so classifier filters are not used.

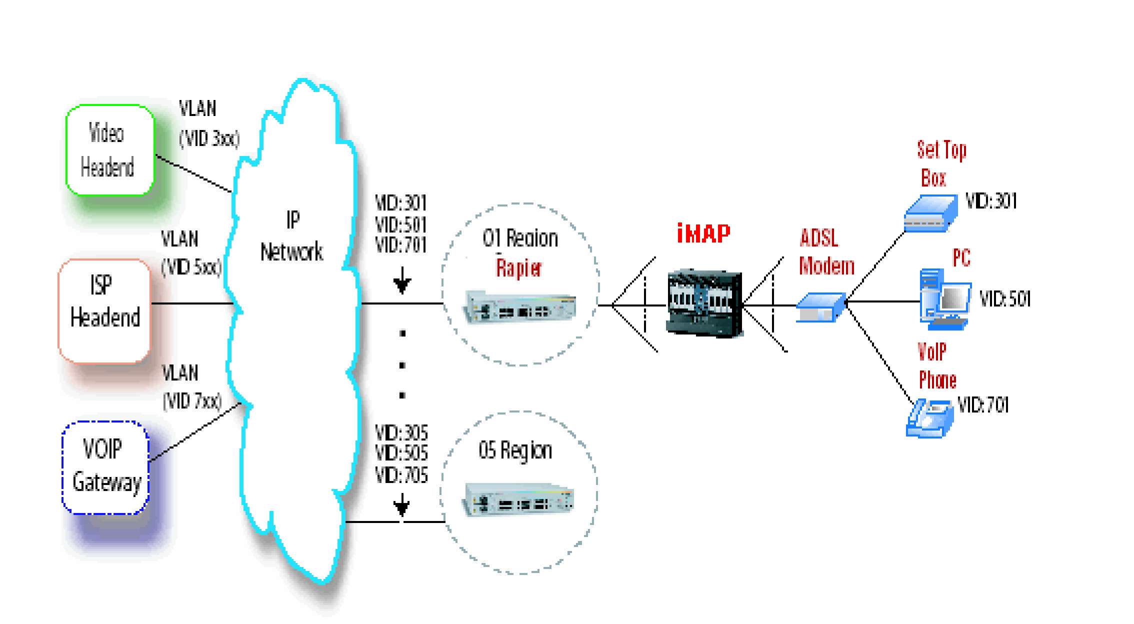


FIGURE 10-8 Sample QoS Network (iMAP MAP Device)

Table 10-11 lists the quality attributes for these classes of service.:

TABLE 10-11 Classes of Service for a Subscriber

Class of Service	Application	Delay	Jitter	Packet Loss
qos_voice	Voice	Low	Low	Low
qos_video	Video	Low	Undefined	Low
qos_data	internet access	Undefined	Undefined	Low
default	Non-critical	Undefined	Undefined	Undefined

- For qos_voice, the subscriber is set up on a VLAN with the VID 701, and the voice traffic is the only incoming stream with a VLAN tag; all other traffic is untagged and is given a tag by its port association.
- For qos_data the subscriber is set up on a VLAN with VID 501.
- For qos_video the subscriber is set up on a VLAN with VID 301, and will connect to the subscriber's Set Top Box (STB).

10.9.1 Creating the QoS Policy Flow

The QoS Policy Flow will be used to create the names for these flows. Following are the steps to create a flow for qos_voice:

1. Click on the Network Services menu and select *Create/Edit QoS Configuration -> Create/Edit Flows*
2. The QOS Policy Flow Dialog window appears.
3. Click on **New Flow** and enter *qos_voice* as the New Name, then **Select**.
4. The Edit QOS Device Class List appears. Select **Telesyn** only, then **Select**.
5. The default classifier (ETHFORMAT=ANY) appears in the Flow Classifiers list. Change this as follows:
   1. In the Classifier attribute pull-down, select VID
   2. A blank field appears next to VID with a default classifier number. Replace with 701.
   3. Click on **Click Here to Add or Replace Parameter**. The default Classifier is replaced with the VID=701 classifier.
6. Click on Save Flow and OK to confirm. This saves the Policy Flow name qos_voice, and this will appear in pull-downs of Flow Names where appropriate.
7. Repeat this and create qos_data, qos_video, and [All Packets]. When creating these, you can click on the Copy Flow qos_voice tic box so that the VID attribute is copied over. You then replace the VID numbers.

10.9.2 Creating the QoS Priority Actions

The QoS Priority Action will be used to create the names for these actions. Following are the steps to create a priority action for qos_voice:

1. Click on the Network Services menu and select *Create/Edit QoS Configuration -> Create/Edit Priority Actions*
2. The QOS Priority Action Form appears.
3. Click on **New Action** and enter *voice_priority* as the New Name, then **Select**.
4. The Edit QOS Device Class List appears. Select **Telesyn** only, then **Select**.
5. The default priority (FORWARD) appears in the Flow Classifiers list. Change this as follows:
   1. In the Priority attribute pull-down, select SETVPRIORITY
   2. A blank field appears next to SETVPRIORITY with a default number (0). Replace with 7.
   3. Click on **Click Here to Add or Replace Parameter**. The default Priority is added to the FORWARD action.
   4. Click on the FORWARD action and select **Delete**. Now SETVPRIORITY is the only action parameter.
6. Click on **Save Priority Action** and **OK** to confirm. This saves the Priority Action name *voice_priority*, and this will appear in pull-downs of Priority Action where appropriate.
7. Repeat this and create data_priority, video_priority, and [No Action]. When creating these, you can click on the Copy from Action voice-priority tic box so that the SETVPRIORITY is copied over. You then replace the SETVPRIORITY numbers.

10.9.3 Creating the QoS Traffic Actions

The QoS Traffic Actions will be used to create the names for these traffic actions. Following are the steps to create a traffic action limit_voice.

1. Click on the Network Services menu and select *Create/Edit QoS Configuration -> Create/Edit Traffic Actions*
2. The QOS Traffic Action Form appears.
3. Click on **New Action** and enter *limit_voice* as the New Name, then **Select**.
4. The Edit QOS Device Class List appears. Select **Telesyn** only, then **Select**.
5. The default actions (RATE and BURSTSIZE) appear in the Traffic Action Parameters list. Change this as follows:

1. Rate and Burstrate parameters are initially in square brackets and colored red. This is because the default values will not work for both 7000 and 9000 devices, but the parameters are required. This keeps the user from inadvertently saving the Actions without looking at these parameters and consciously setting their values
2. With the RATE parameter, select RATE from the pull-down. In the blank filed, enter 1000.
3. Click on **Click Here to Add or Replace Parameter**. The default RATE is replaced with the new value.
4. Repeat these steps with the BURSTSIZE parameter, selecting the pull-down 32KB.
5. In the pull-down of parameters, select NCCOUNT. The option ON or OFF appears in a pull-down. Select ON.
6. Click on **Click Here to Add or Replace Parameter**. This adds the NCOUNT parameter to the list.

6. Click on **Save Traffic Action** and **OK** to confirm. This saves the Traffic Action name qos_voice, and this will appear in pull-downs of Traffic Action Names where appropriate.
7. Since there are no other traffic actions to create for this flow, **Close** the Form.

10.9.4 Creating the Policy and its Rules

The policy can now be created, since it is now possible to set up the rules that make up the policy.

1. Click on the Network Services menu and select *Create/Edit QoS Configuration -> Create/Edit Policies.*
2. The QOS Policy Maintenance window appears.
3. Click on **New Policy** and enter *tripleplay* as the New Name, then **Select**. (Note that entering a name such as triple_play will bring up an error since this includes an underscore.)
4. The Edit QOS Device Class List appears. Select **Telesyn** only, then **Select**.
5. Enter a description for what the policy will do, since the name may not be descriptive enough.
6. The traffic rules can now be added. Under Row Operations, select **Add Rule**. The **QOS Policy Rule Form** appears.
7. In the Flow pull-down, which should have the default **[All Packets]**, select qos_voice. In the Priority pull-down, which should have the default [No Action], select **voice_priority.**
8. Click on Add. This puts the flow and priority in a row and associates them. Select the Traffic Action limit_voice. with a traffic action.
9. If this is correct, select Add Rule. This will add the rule to the tripleplay policy.
10. Add rules that associate the other attributes (qos_data/data_priority, qos_video/video_priority). Each rule is defined starting with selecting the Add Rule button in Step 6
11. Select Save Policy to make the policy permanent.
12. Once the policy exists, it can be viewed by selecting the QoS Policies Tree. The Packet Flows and Actions can also be viewed by selecting their nodes.

10.10 Example of a Rapier/SwitchBlade Policy

Figure 10-9 shows a policy, called enterprise, that was created for a business that has the following needs:

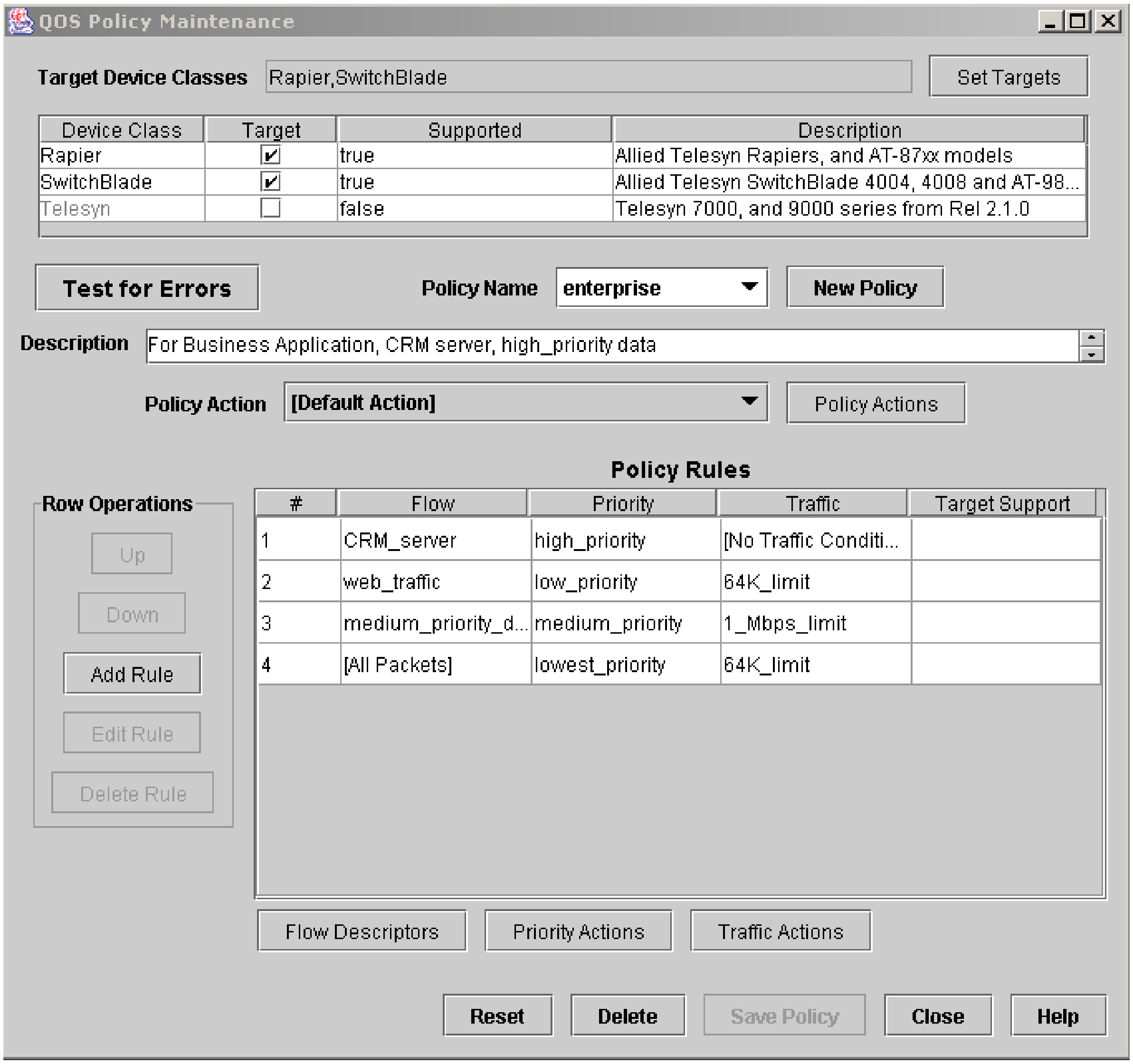
- There is a server (CRM) in which all traffic sent from and to this server (using the IP address) has the highest priority. This is done since many business applications may involve web-based data, video conferencing, email, etc. and so all traffic types using this server will have the highest priority. There is no traffic conditioning, so all available bandwidth will be used.
- Web traffic (TCP/IP over port 80) will be handled with separate rule. When a packet comes in that is not using the IP address of the CRM server, but uses TCP/IP over port 80, it will be placed in a low priority queue (1) and set to a maximum bandwidth of 64Kbps.
- Data that does not use the CRM server IP address and is not web-based, but has a certain level of service (DSCP=55) is placed in a queue that has a priority higher than web traffic, but lower than the CRM server. It can use bandwidth up to 1Mbps, after which packets are dropped. (It is assumed that this bandwidth is sufficient for most applications.)

- All other traffic is placed in the lowest priority queue and has, like web-based traffic, a maximum bandwidth of 64Kbps. It therefore uses the same traffic action.

Figure 10-10 through Figure 10-14 shows how the forms are datafilled to define the flows, priorities, and actions.

Following are notes on using these forms:

- A flow, priority, or action can be defined first and made applicable to **all** device types. In creating a policy, the user can control which device types a flow, priority, or action will apply to.
- The user can create the flows, priorities, and actions first, and then in creating the policy create the rules that associate these together.
- The user can create a policy first, and then use the **Flow Descriptors**, **Priority Actions**, and **Traffic Actions** buttons to create new flows, priorities, and actions before defining the Rule Table.
- The **Copy** and **Paste** buttons are useful when, in defining a flow, priority, or action, the user needs to copy over the attributes to the other devices. An example would be in defining the flow CRM server; the user could define the attributes for one device type, and then copy and paste these for the other device types.



Target Device Classes: Rapier,SwitchBlade

Device Class	Target	Supported	Description
Rapier	☑	true	Allied Telesyn Rapiers, and AT-87xx models
SwitchBlade	☑	true	Allied Telesyn SwitchBlade 4004, 4008 and AT-98...
Telesyn	□	false	Telesyn 7000, and 9000 series from Rel 2.1.0

Policy Name: enterprise

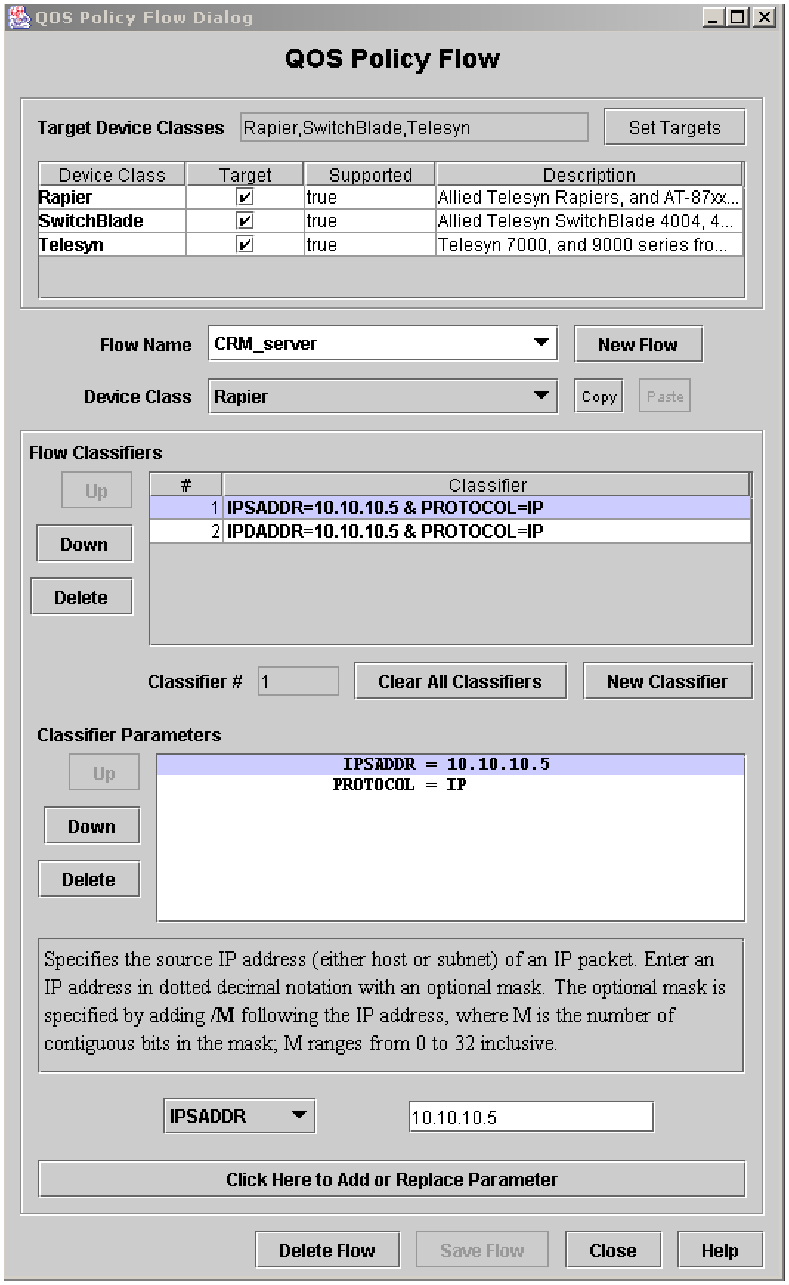
Description: For Business Application, CRM server, high_priority data

Policy Action: [Default Action]

Policy Rules

#	Flow	Priority	Traffic	Target Support
1	CRM_server	high_priority	[No Traffic Conditi...	
2	web_traffic	low_priority	64K_limit	
3	medium_priority_d...	medium_priority	1_Mbps_limit	
4	[All Packets]	lowest_priority	64K_limit	

FIGURE 10-9 Example Policy for Rapier/SwitchBlade Devices



Target Device Classes: Rapier,SwitchBlade,Telesyn

Device Class	Target	Supported	Description
Rapier	☑	true	Allied Telesyn Rapiers, and AT-87xx...
SwitchBlade	☑	true	Allied Telesyn SwitchBlade 4004, 4...
Telesyn	☑	true	Telesyn 7000, and 9000 series fro...

Flow Name: CRM_server

Device Class: Rapier

#	Classifier
1	IPSADDR=10.10.10.5 & PROTOCOL=IP
2	IPDADDR=10.10.10.5 & PROTOCOL=IP

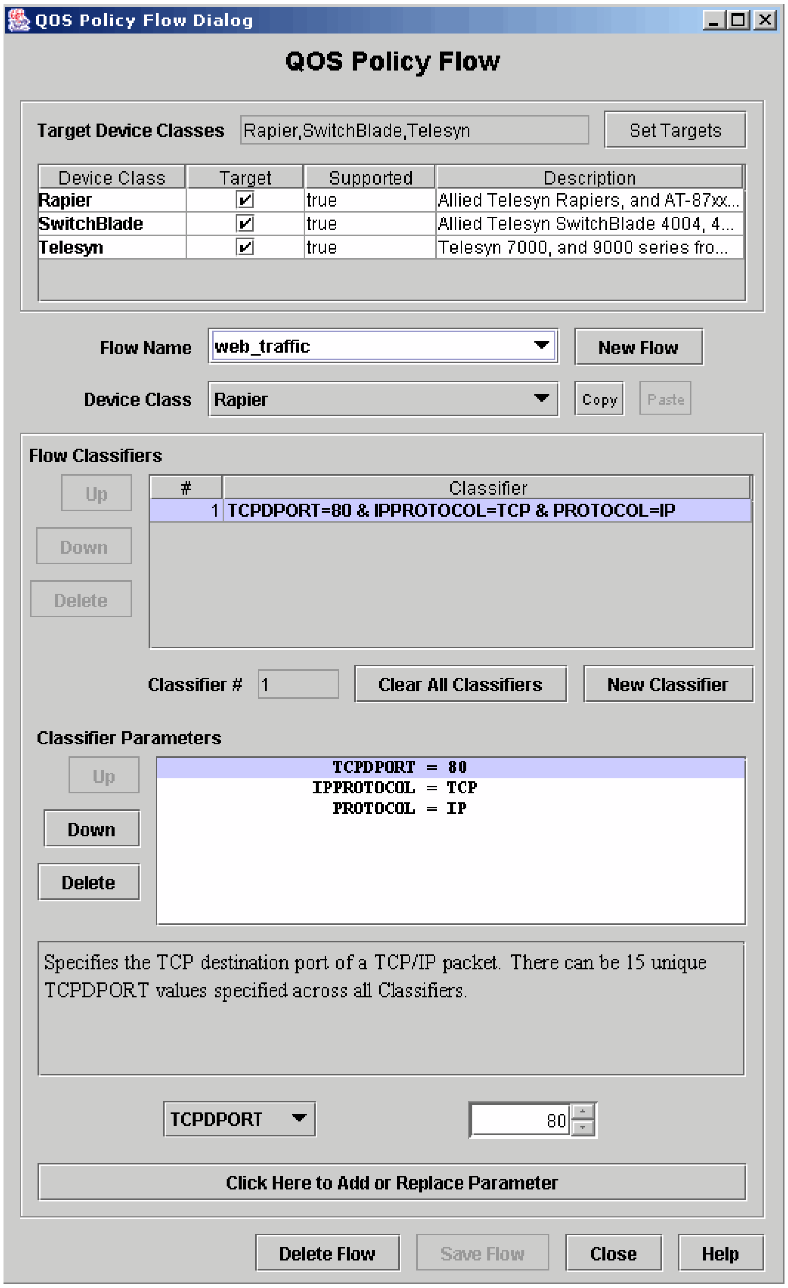
Classifier #: 1

```
IPSADDR = 10.10.10.5
PROTOCOL = IP
```

Specifies the source IP address (either host or subnet) of an IP packet. Enter an IP address in dotted decimal notation with an optional mask. The optional mask is specified by adding /M following the IP address, where M is the number of contiguous bits in the mask; M ranges from 0 to 32 inclusive.

IPSADDR: 10.10.10.5

FIGURE 10-10 QoS Flow for enterprise Policy (CRM server)



QOS Policy Flow

Target Device Classes: Rapier,SwitchBlade,Telesyn

Device Class	Target	Supported	Description
Rapier	☑	true	Allied Telesyn Rapiers, and AT-87xx...
SwitchBlade	☑	true	Allied Telesyn SwitchBlade 4004, 4...
Telesyn	☑	true	Telesyn 7000, and 9000 series fro...

Flow Name: web_traffic

Device Class: Rapier

Flow Classifiers

#	Classifier
1	TCPDPORT=80 & IPPROTOCOL=TCP & PROTOCOL=IP

Classifier #: 1

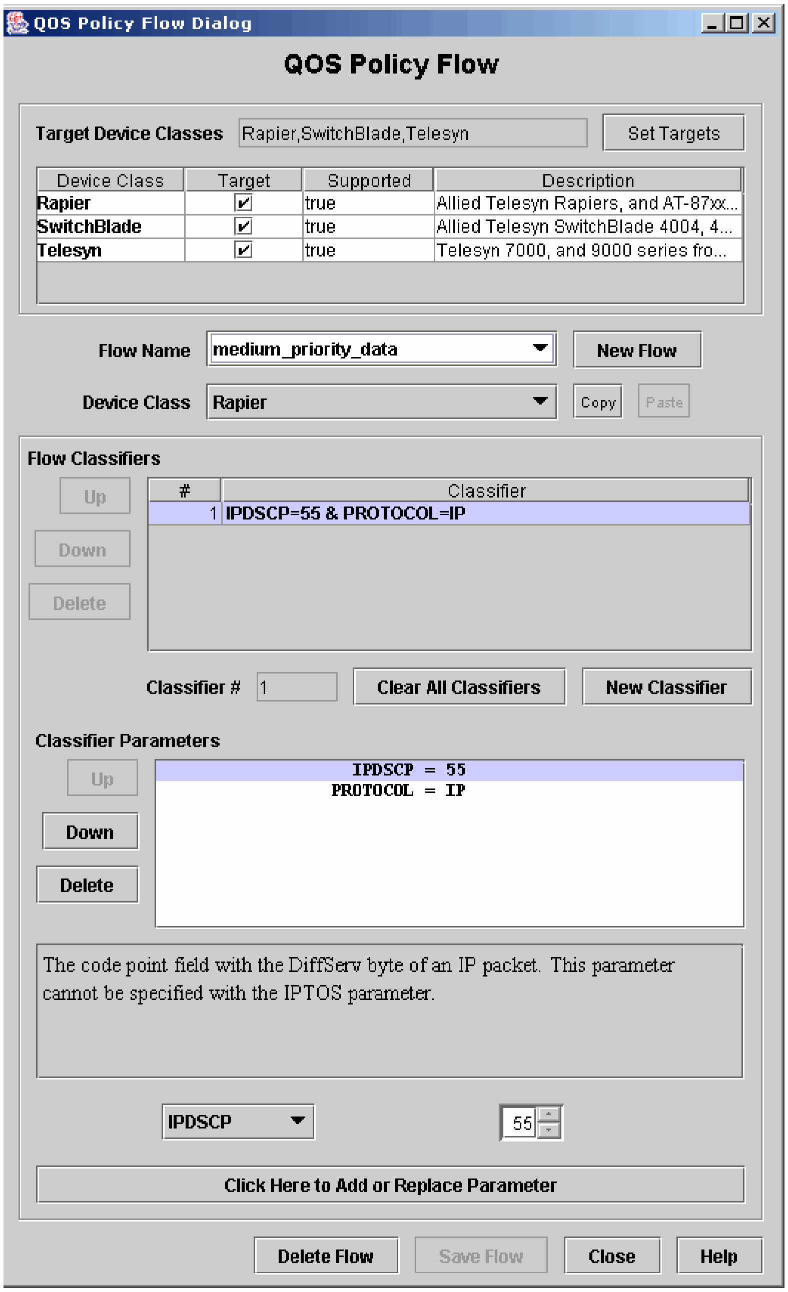
Classifier Parameters

```
  TCPDPORT  = 80
IPPROTOCOL  = TCP
  PROTOCOL  = IP
```

Specifies the TCP destination port of a TCP/IP packet. There can be 15 unique TCPDPORT values specified across all Classifiers.

TCPDPORT: 80

FIGURE 10-11 QoS Flow for enterprise Policy (web_traffic)



QOS Policy Flow

Target Device Classes: Rapier,SwitchBlade,Telesyn

Device Class	Target	Supported	Description
Rapier	☑	true	Allied Telesyn Rapiers, and AT-87xx...
SwitchBlade	☑	true	Allied Telesyn SwitchBlade 4004, 4...
Telesyn	☑	true	Telesyn 7000, and 9000 series fro...

Flow Name: medium_priority_data

Device Class: Rapier

Flow Classifiers

#	Classifier
1	IPDSCP=55 & PROTOCOL=IP

Classifier # 1

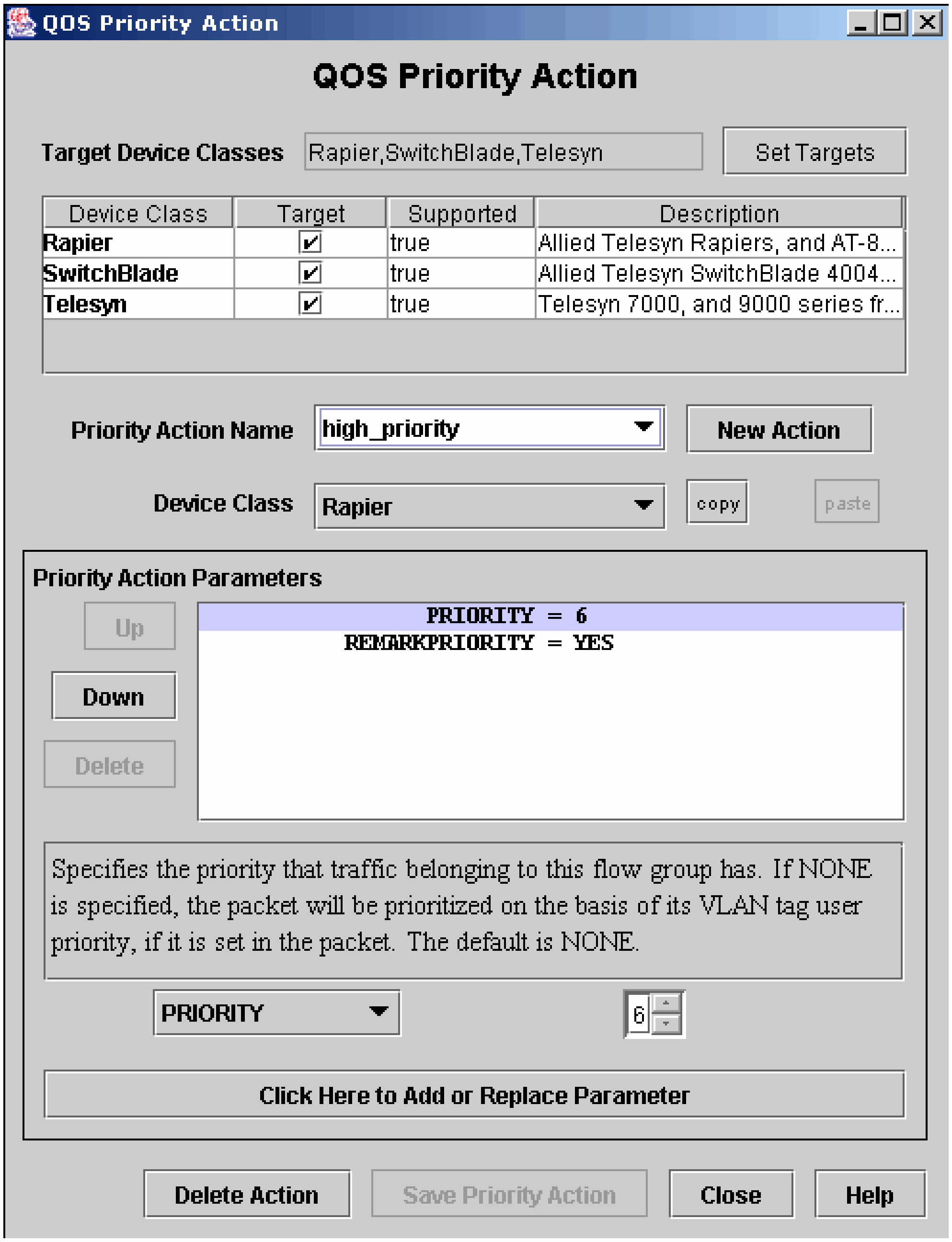
Classifier Parameters

```
IPDSCP  = 55
PROTOCOL  = IP
```

The code point field with the DiffServ byte of an IP packet. This parameter cannot be specified with the IPTOS parameter.

IPDSCP 55

FIGURE 10-12 QoS Flow for enterprise Policy (medium_priority_data)



QOS Priority Action

Target Device Classes: Rapier,SwitchBlade,Telesyn

Device Class	Target	Supported	Description
Rapier	☑	true	Allied Telesyn Rapiers, and AT-8...
SwitchBlade	☑	true	Allied Telesyn SwitchBlade 4004...
Telesyn	☑	true	Telesyn 7000, and 9000 series fr...

Priority Action Name: high_priority

Device Class: Rapier

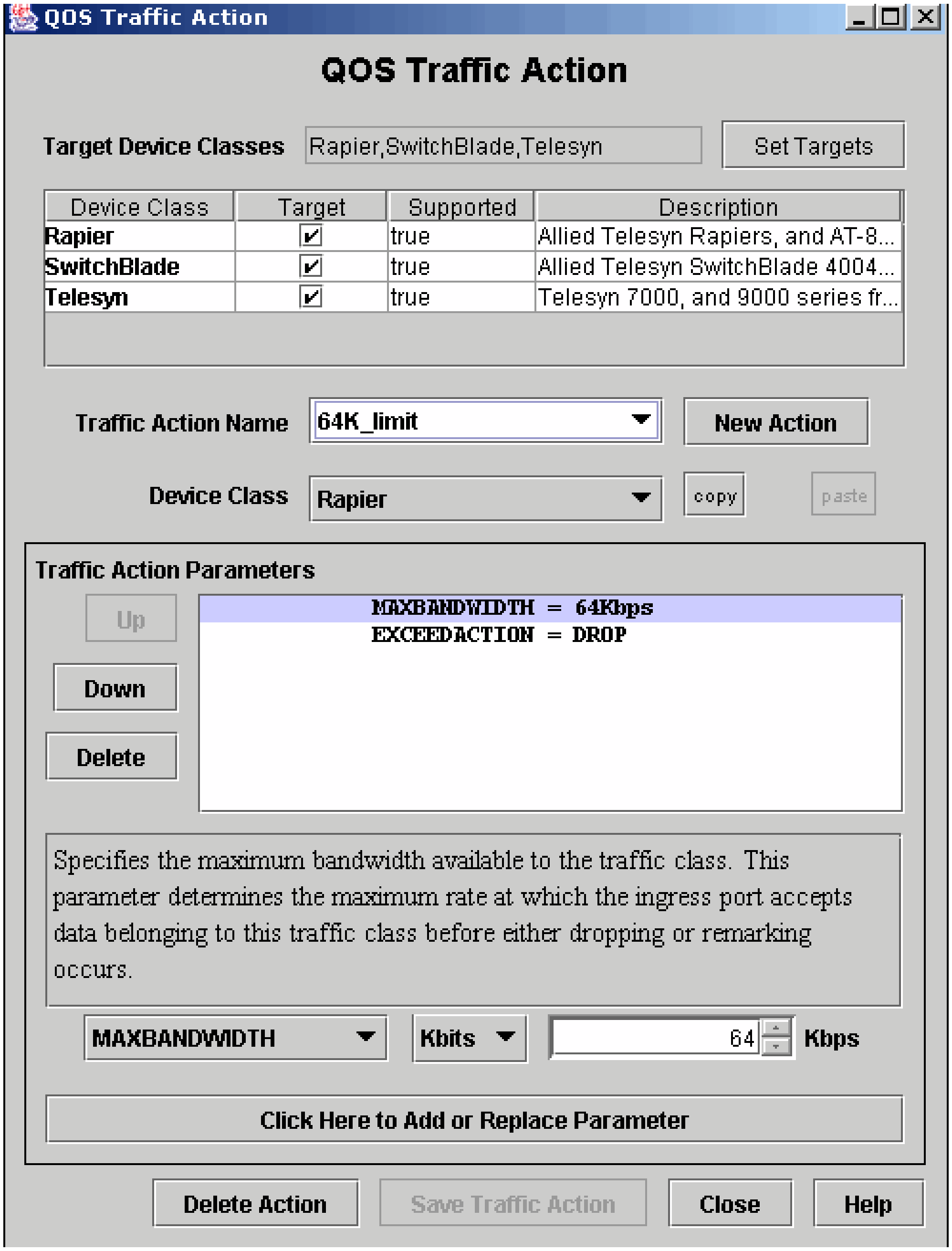
Priority Action Parameters

```
PRIORITY = 6
REMARKPRIORITY = YES
```

Specifies the priority that traffic belonging to this flow group has. If NONE is specified, the packet will be prioritized on the basis of its VLAN tag user priority, if it is set in the packet. The default is NONE.

PRIORITY: 6

FIGURE 10-13 QoS Priority for enterprise Policy (high_priority)



QOS Traffic Action

Target Device Classes: Rapier,SwitchBlade,Telesyn

Device Class	Target	Supported	Description
Rapier	☑	true	Allied Telesyn Rapiers, and AT-8...
SwitchBlade	☑	true	Allied Telesyn SwitchBlade 4004...
Telesyn	☑	true	Telesyn 7000, and 9000 series fr...

Traffic Action Name: 64K_limit

Device Class: Rapier

Traffic Action Parameters

```
MAXBANDWIDTH = 64Kbps
EXCEEDACTION = DROP
```

Specifies the maximum bandwidth available to the traffic class. This parameter determines the maximum rate at which the ingress port accepts data belonging to this traffic class before either dropping or remarking occurs.

MAXBANDWIDTH Kbits 64 Kbps

FIGURE 10-14 QoS Traffic for enterprise Policy (64K_limit)

10.11 Example of an EPON/ONU Interface Policy

Creating policies for the EPON/ONU involves the same steps as creating policies for the various device types, but the administrator should understand the EPON/ONU interfaces and how policies work on these interfaces.

Note: *Refer to the Software Reference for iMAP Series Switches for complete information about provisioning the components that make up the EPON configuration.*

Following are the components that make the EPON/ONU interfaces:

- EPON Interface - The EPON interface is one-to-one with the physical EPON port on the card. Like other interfaces the system can raise alarms on it, collect statistics on it, enable/disable it, etc. It will host ONU interfaces but it does not support any ETH interfaces directly.

  The EPON interface is always present when the card is present (i.e. they are not created/deleted by the user). The EPON interface is identified as an interface like epon:4.1 with the slot and physical port as the indices.

  The EPON interface has IGMP-specific attributes for video multicasting:

  - The VLAN for IP Multicast
  - IP Source Address for IGMP Proxy (0.0.0.0 is the default; refer to the *Software Reference for iMAP Series Switches* on using other addresses).
- ONU (Included with iMG/RG)

The ONU interface supports/hosts one (and only one) ETH interface, which is actually an Ethernet port inside the iMG/RG. The ONU interface is identified like “onu:4.1.7” with the EPON's slot and physical port as the first two indices. The last index is a logical identifier.

- SLA / QOSPOLICY (VLAN basis)

The SLA provides attributes to ensure that a traffic flow is given adequate bandwidth to support a service on an ONU. Since the service may involve downstream only or upstream/downstream data flows, the QOSPOLICY has both upstream and downstream attributes.

The QOSPOLICY is associated with a VLAN as well, and so to configure the QOSPOLICY, the user must understand the VLANs associated with a service and the traffic flows (upstream/downstream and downstream only) for each type of service.

There are two types of traffic flows on which QOSPOLICYs are configured:

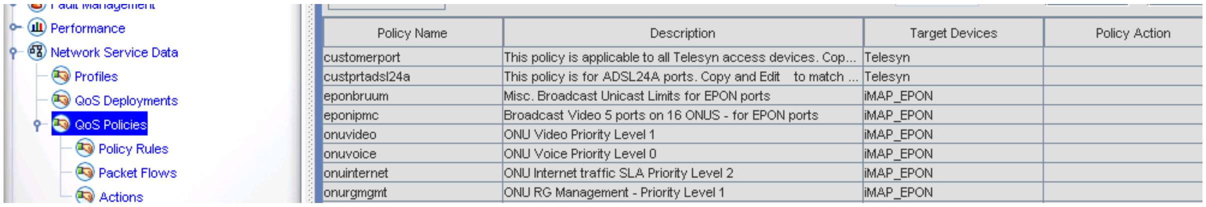
1. Upstream/Downstream Links
   - There is one or more per ONU
   - Each one carries **one** VLAN to **one** ONU.
   - Downstream, they carry known unicast packets to the ONU
   - Upstream, they carry unicast, broadcast, multicast, and unknown MAC packets.
   - The first one provisioned on the ONU carries some control and management traffic upstream
2. Downstream Only Link
   - One is for all ONUs
   - Carries two types of traffic, with each having a separately defined SLA (and therefore QOSPOLICY)

     - Multicast traffic for only the IP Multicast (IPMC) VLAN

     - Broadcast, Unknown Unicast, and flooded Multicast (BRUUM). This downstream link is shared for all VLANs on all ONUs on the EPON.

When the AlliedView NMS is first loaded, a set of polices (with their flows, priorities, and traffic actions) are included. These profiles as well as the relevant VLAN can then be included with EPON and ONU port profiles.

The following figure shows the default profiles, followed by a table that describes the attributes of these policies.



Policy Name	Description	Target Devices	Policy Action
customerport	This policy is applicable to all Telesyn access devices. Cop...	Telesyn	
custprtadsl24a	This policy is for ADSL24A ports. Copy and Edit to match ...	Telesyn	
eponbruum	Misc. Broadcast Unicast Limits for EPON ports	iMAP_EPON	
eponipmc	Broadcast Video 5 ports on 16 ONUS - for EPON ports	iMAP_EPON	
onuvideo	ONU Video Priority Level 1	iMAP_EPON	
onuvoice	ONU Voice Priority Level 0	iMAP_EPON	
onuinternet	ONU Internet traffic SLA Priority Level 2	iMAP_EPON	
onurgmgmt	ONU RG Management - Priority Level 1	iMAP_EPON	

FIGURE 10-15 Default EPON and ONU QoS Policies

TABLE 10-12 QoS Flows for EPON Interfaces

Flow	Classifier Parameters	Notes
IpFilterFlow	IPSADDR=<ALLOWED_IPS> &PROTOCOL=IP	
onuflow	ETHFORMAT=ANY	

TABLE 10-13 QoS Actions for EPON Interfaces

Flow	Action Parameters	Notes

EPON_BRUUM	MINDOWNSTREAMRATE=1M;
	MAXDOWNSTREAMRATE=2M;
	DOWNDELAYSENSITIVITY=TOLERANT
	DOWNBURSTSIZE=10K	

EPON_IPMC	MINUPSTREAMRATE=0
	MAXDOWNSTREAMRATE=1G;
	DOWNBURSTSIZE=256K
	DOWNDELAYSENSITIVITY=TOLERANT
	MINDOWNSTREAMRATE=1M;	

TABLE 10-14 QoS Actions for ONU Interfaces

Flow	Action Parameters	Notes

ONU_INTERNET	MINDOWNSTREAMRATE=0K
	MAXDOWNSTREAMRATE=4M
	DOWNDELAYSENSITIVITY=TOLERANT
	DOWNBURSTSIZE=5K
	MINUPSTREAMRATE=1M
	MAXUPSTREAMRATE=2M
	UPDELAYSENSITIVITY=TOLERANT
	UPBURSTSIZE=3K	

ONU_VIDEO	MINDOWNSTREAMRATE=20M
	MAXDOWNSTREAMRATE=512M
	DOWNDELAYSENSITIVITY=TOLERANT
	DOWNBURSTSIZE=30K
	MINUPSTREAMRATE=128K
	MAXUPSTREAMRATE=256K
	UPDELAYSENSITIVITY=TOLERANT
	UPBURSTSIZE=3K;	

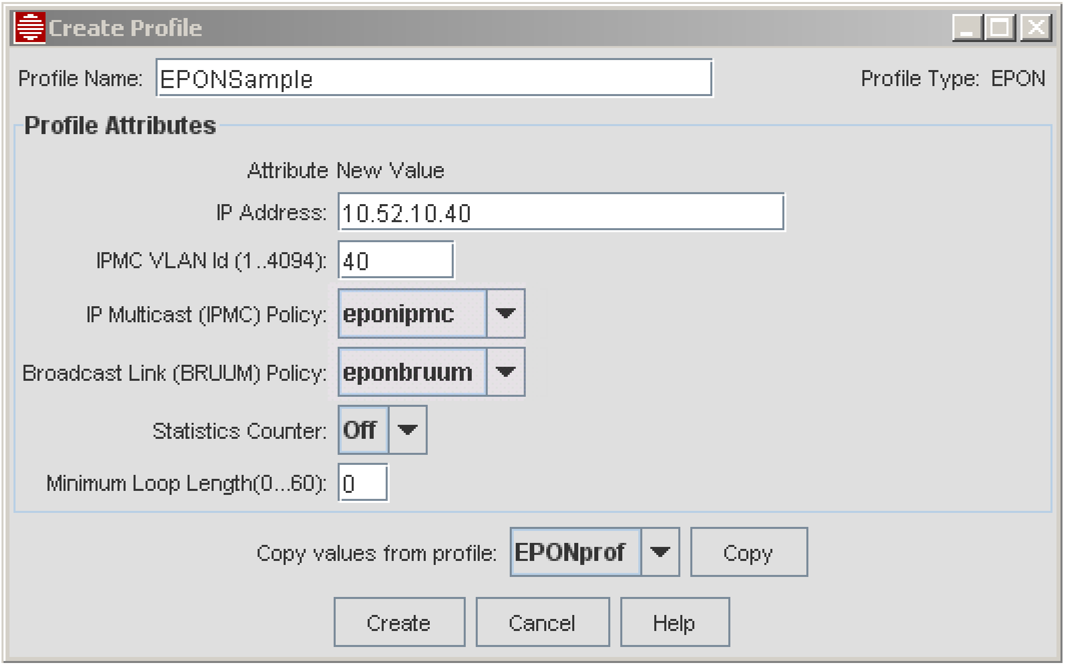
ONU_VOICE	MINDOWNSTREAMRATE=512K
	MAXDOWNSTREAMRATE=512K
	DOWNDELAYSENSITIVITY=SENSITIVE
	DOWNBURSTSIZE=8K
	MINUPSTREAMRATE=512K
	MAXUPSTREAMRATE=512K
	UPBURSTSIZE=8K
	UPDELAYSENSITIVITY=TOLERANT	

ONU_RG_MGMT	MINDOWNSTREAMRATE=1M
	MAXDOWNSTREAMRATE=256M
	DOWNDELAYSENSITIVITY=TOLERANT
	DOWNBURSTSIZE=30K
	MINUPSTREAMRATE=1K
	MAXUPSTREAMRATE=64K
	UPDELAYSENSITIVITY=TOLERANT
	UPBURSTSIZE=1K	

TABLE 10-15 Default QoS Policies for EPON and ONU Interfaces

Policy	Flow	Priority	Action	Notes
eponbruum	IpFilterFlow	Allow	None	
	AnyOtherIp	Deny	None	
	AllPackets	ONUPriority	EPON_BRUUM	
eponipmc	IpFilterFlow	Allow	None	
	AnyOtherIp	Deny	None	
	AllPackets	ONUPriority	EPON_IPMC	
onuvideo	IpFilterFlow	Allow	None	
	AnyOtherIp	Deny	None	
	AllPackets	ONUPriority	ONU_VIDEO	
onuvoice	IpFilterFlow	Allow	None	
	AnyOtherIp	Deny	None	
	AllPackets	ONUPriority	ONU_VOICE	
oneinternet	IpFilterFlow	Allow	None	
	AnyOtherIp	Deny	None	
	AllPackets	ONUPriority	ONU_INTERNET	
onurgmgmt	IpFilterFlow	Allow	None	
	AnyOtherIp	Deny	None	
	AllPackets	ONUPriority	ONU_RG_MGMT	

With these policies, the administrator can these include these with the profiles for the EPON and ONU ports.



Profile Name: EPONSample

Profile Type: EPON

Profile Attributes

Attribute New Value

IP Address: 10.52.10.40

IPMC VLAN Id (1..4094): 40

IP Multicast (IPMC) Policy: eponipmc

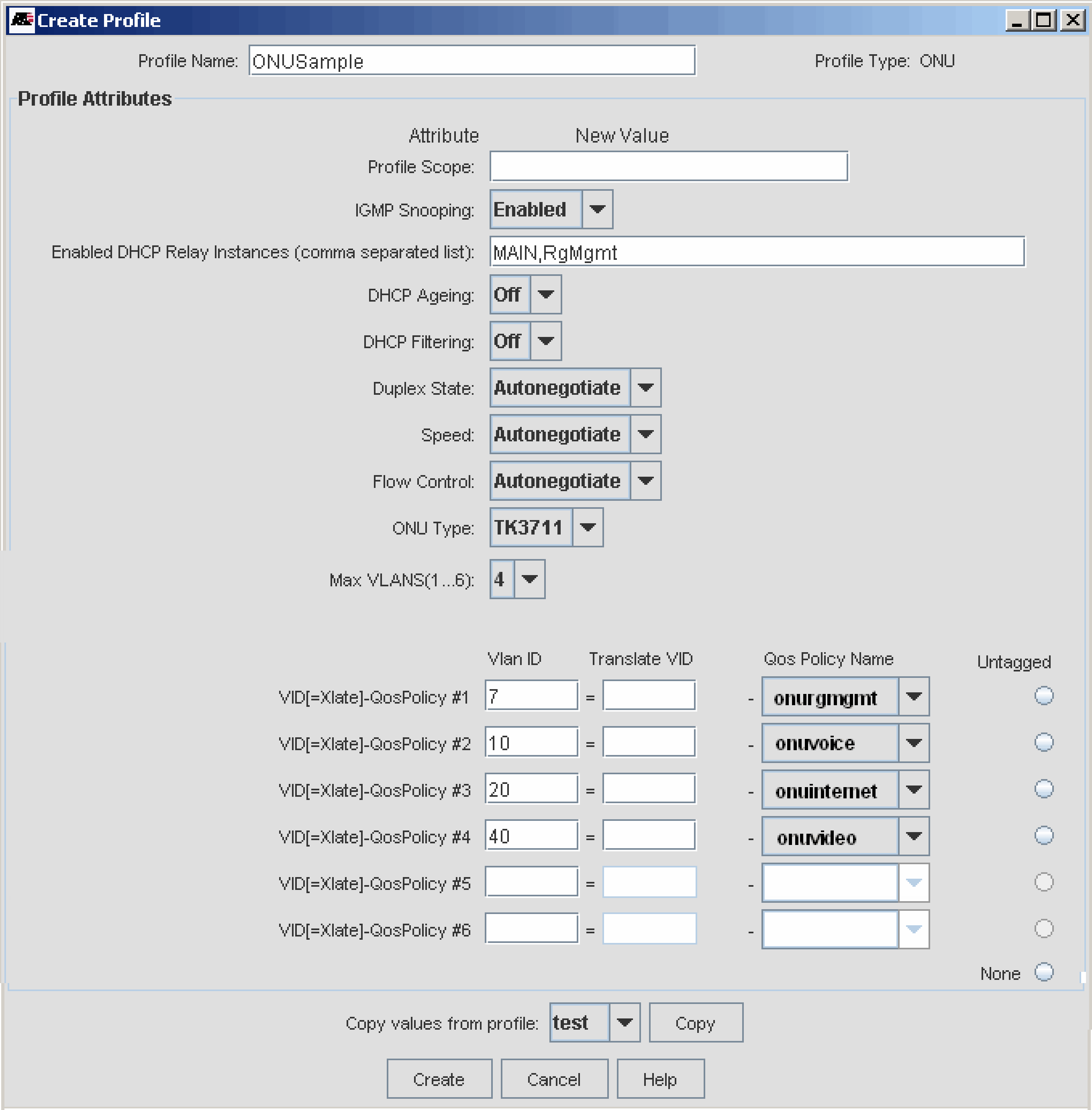
Broadcast Link (BRUUM) Policy: eponbruum

Statistics Counter: Off

Minimum Loop Length(0...60): 0

Copy values from profile: EPONprof

FIGURE 10-16 Example EPON Port Profile



Create Profile

Profile Name: ONUSample

Profile Type: ONU

Profile Attributes

Attribute	New Value
Profile Scope:	
IGMP Snooping:	Enabled
Enabled DHCP Relay Instances (comma separated list):	MAIN,RgMgmt
DHCP Ageing:	Off
DHCP Filtering:	Off
Duplex State:	Autonegotiate
Speed:	Autonegotiate
Flow Control:	Autonegotiate
ONU Type:	TK3711
Max VLANS(1...6):	4

	Vlan ID		Translate VID		Qos Policy Name	Untagged
VID[=Xlate]-QosPolicy #1	7	=		-	onurgmgmt	○
VID[=Xlate]-QosPolicy #2	10	=		-	onuvoice	○
VID[=Xlate]-QosPolicy #3	20	=		-	onuinternet	○
VID[=Xlate]-QosPolicy #4	40	=		-	onuvideo	○
VID[=Xlate]-QosPolicy #5		=		-		○
VID[=Xlate]-QosPolicy #6		=		-		○
					None	○

Copy values from profile: test

FIGURE 10-17 Example ONU Port Profile

Note: *The administrator can also create and view QoS policies using the CLI. When policies are created by the AlliedView NMS, they are shown at the CLI with the prefix "NMS_" added and may append an "_a" or "_b" to the name. When policies that are created at the CLI, they appear on the ONU and EPON port details screens with a question mark appended.*

Note: *Any existing ONU or EPON profiles have a '?' appended to the profile name. Administrators can continue to use these profiles and they will work as they did in 8.0. However, if you edit a profile or create a new one, only the 'NMS Qos Policy names' can be selected, forcing an upgrade for these Profiles.*

Note: *In release 10.0 SP2, the EPON supports VLAN translations. As a result, the translated VLAN ID is also included as part of setting the QOS policies.*

10.12 QoSPolicies for the FX20 Interface

10.12.1 Overview

The NMS GUI for QoS allows you to configure ingress traffic parameters on the iMAP ports.

You can set the priority of traffic packets for the entire iMAP by setting the priority (usually through VLANs) and mapping them to system-wide queues before forwarding. (This is done on the NMS by creating a profile for the Allied Telesis device. By doing this, the administrator can set a queue number (0 = lowest priority; higher numbers = higher priority) and match it to the p-bit value in the packet.

In the 11.0 release of iMAP software, there was an enhancement to provisioning egress interfaces for the FX20 interfaces; a QosPolicy, which defines data stream attributes, could be associated with a **specific queue** on the FX20 interface. This was an enhancement over other interfaces, where rate and burst attributes are defined for the entire interface (when using the attribute EGRESSLIMITER), or where a QOSPOLICY defined data stream attributes on a VLAN basis (when provisioning EPON).

On the NMS, there is already a GUI framework for creating the QoS Policies for the EPON/ONU configuration, as detailed in "Example of an EPON/ONU Interface Policy" on page 253.

In NMS 11.0 SP4, this FX20 QoS feature is added; using (for the most part) the NMS GUI that is used to configure QoSPolicies, the administrator can engineer traffic going through the FX20 by creating an NMS Policy that is a set of QosPolicies that tie together the queues and their data stream attributes. This policy is then included in a Profile that is for the FX20 port. The same QosPolicy can be shared with multiple ports and queues since the configuration is applied on a per port and per queue basis.

The following figure summarizes this feature. The iMG/RG is connected to the iMAP over an FX20 interface. Packets from the network have a priority based on service (usually set through VLANs), and the iMAP-level profile will map the priorities to queues. At the egress for an FX20 interface, a QoSPolicy is made up of a set of rules that tie together for each queue the attributes of its data stream.

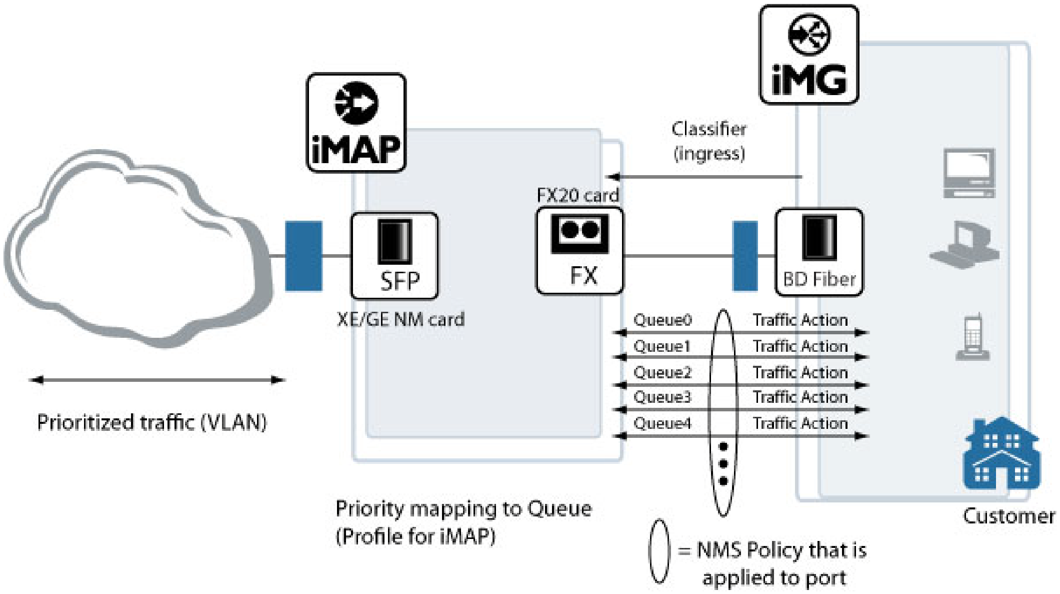


FIGURE 10-18 Summary of FX20 QoS per Queue Feature

10.12.2 Overview of GUI

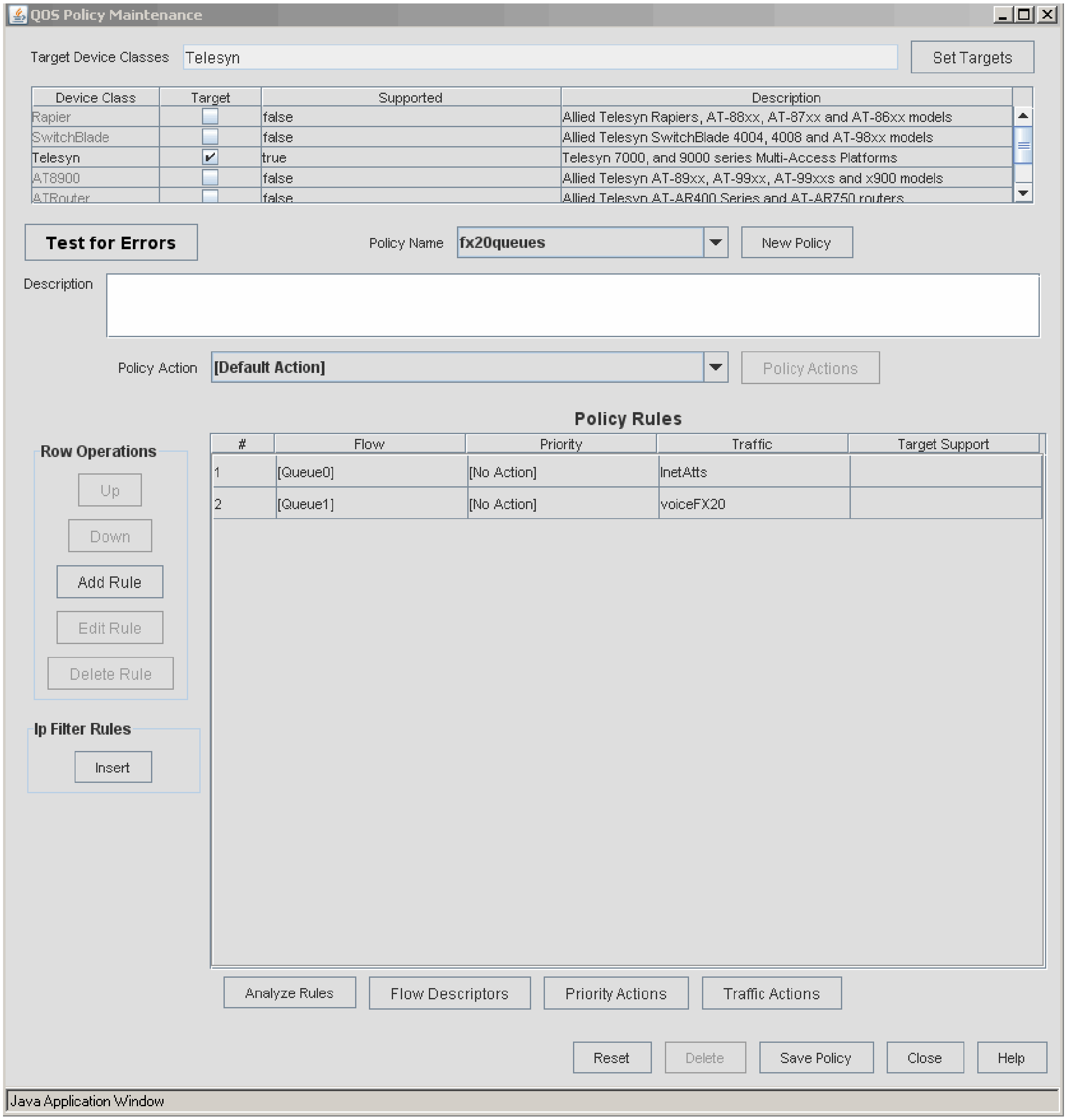
This feature uses the GUI framework that is used to configure SLA bandwidth parameters for ONU interfaces, as detailed in "Example of an EPON/ONU Interface Policy" on page 253, but instead of defining QoSPolicies for each VLAN on an ONU, an NMS Policy consists of a set of rules in which each rule maps a queue to a specific traffic action. The GUI is updated as follows when creating a rule:

- QoS Packet Flow - Each flow represents a queue, and there are already in the pull-down for flows the selections for queues, **[Queue0]** through **[Queue7].**
- Traffic Priority - The rules that make up a QoSPolicy for the FX20 do not use these (if the administrator chooses a Queue for a Flow, and then a Priority, the Priority will be ignored).
- Combining classifier and FX20 interface Rules - For traffic control that is not part of the FX20 interface feature, rules can still be defined for the interface. However, the same policy rule should not be used for a queue and classifiers when specifying the flow for traffic action.

10.12.3 Example Configuration

The following figure shows a QoSPolicy that reflects the FX20 Egress Queue feature. The rest of this section shows how to configure this QoSPolicy and associate it with an Ether-like port Profile.

Note: With the GUI, there are alternate ways to create the QosPolicy; this is one example.



Target Device Classes: Telesyn

Device Class	Target	Supported	Description
Rapier	□	false	Allied Telesyn Rapiers, AT-88xx, AT-87xx and AT-86xx models
SwitchBlade	□	false	Allied Telesyn SwitchBlade 4004, 4008 and AT-98xx models
Telesyn	☑	true	Telesyn 7000, and 9000 series Multi-Access Platforms
AT8900	□	false	Allied Telesyn AT-89xx, AT-99xx, AT-99xxs and x900 models
ATRouter	□	false	Allied Telesyn AT-AR400 Series and AT-AR750 routers

Policy Name: fx20queues

Description:

Policy Action: [Default Action]

Policy Rules

#	Flow	Priority	Traffic	Target Support
1	[Queue0]	[No Action]	InetAtts	
2	[Queue1]	[No Action]	voiceFX20	

FIGURE 10-19 QoSPolicy or FX20 Egress Queues

1. As mentioned in "Overview of GUI" on page 260, the Traffic Flows are pre-defined and Traffic Priority is not used, so the first step is to create a Traffic Action (or set of Traffic Actions) that will be associated with the queues.

- Select *Network Services -> QoS -> Actions -> Traffic Action* - This brings up the QoS Traffic Action Form.

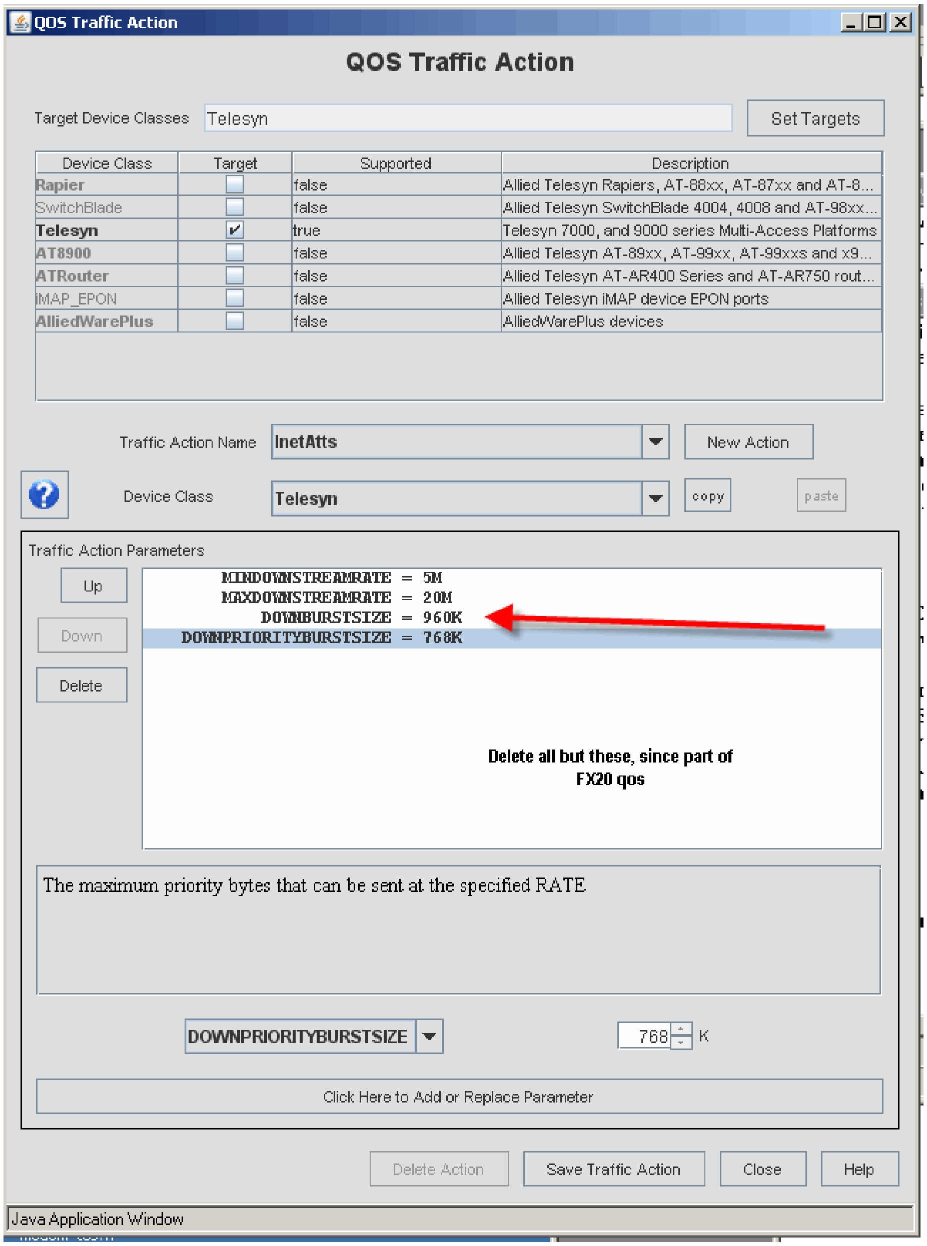
Note: You can also go to the Network Service data node and select QoS policies - Actions, and double click an existing Traffic Action.

- Select the **New Action** button, and enter the New Action Name, following the Policy naming conventions. Do not select the **Copy from ...** tic box.
- At the Edit QoS Device Class List, click on Telesyn and then the **Select** button.

- The QOS Traffic Action form appears with its list of attributes. For the FX20 queue, only four are used, so select these and edit the values.

Note: *Although not necessary, you should delete the other attributes so that only the key attributes are highlighted. Refer to the following figure.*

- Click on **Save Traffic Action**, and click **OK** on the confirmation window.
- Click on **New Action**, enter another Traffic Action name, and select the tic box to copy the attributes from the Traffic Action you just created. You will only need to modify the four attributes and select **Save** to save the second Traffic Action.
- Repeat these steps for each Traffic Action, up to eight.



QOS Traffic Action

Target Device Classes: Telesyn

Device Class	Target	Supported	Description
Rapier	☐	false	Allied Telesyn Rapiers, AT-88xx, AT-87xx and AT-8...
SwitchBlade	☐	false	Allied Telesyn SwitchBlade 4004, 4008 and AT-98xx...
Telesyn	☑	true	Telesyn 7000, and 9000 series Multi-Access Platforms
AT8900	☐	false	Allied Telesyn AT-89xx, AT-99xx, AT-99xxs and x9...
ATRouter	☐	false	Allied Telesyn AT-AR400 Series and AT-AR750 rout...
iMAP_EPON	☐	false	Allied Telesyn iMAP device EPON ports
AlliedWarePlus	☐	false	AlliedWarePlus devices

Traffic Action Name: InetAtts

Device Class: Telesyn

Traffic Action Parameters

```
    MINDOWNSTREAMRATE = 5M
    MAXDOWNSTREAMRATE = 20M
        DOWNBURSTSIZE = 960K
DOWNPRIORITYBURSTSIZE = 768K
```

Delete all but these, since part of FX20 qos

The maximum priority bytes that can be sent at the specified RATE

DOWNPRIORITYBURSTSIZE 768 K

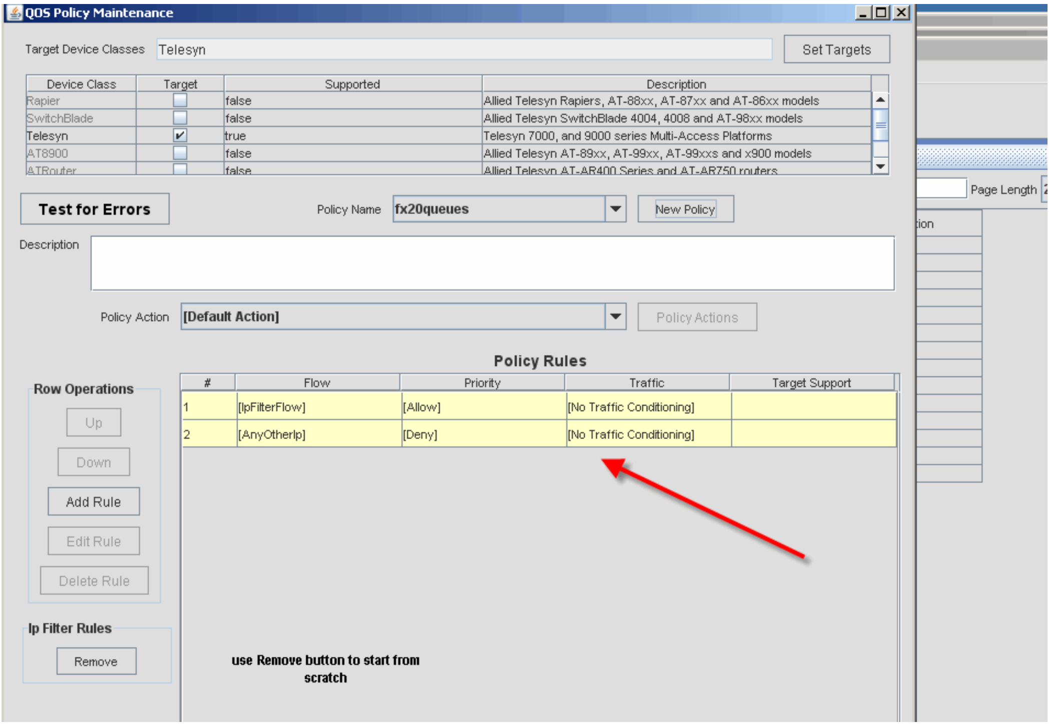
FIGURE 10-20 Creating a Traffic Action for an FX20 Interface Queue

2. With the Traffic Actions created, the QosPolicy (with its set of Rules) can be created.

- Select *Network Services* -> *QoS* -> *Policy* - This brings up the QoS Policy Maintenance Form.

Note: *You can also go to the Network Service data node and select QoS policies -> Actions, and select an existing Policy*

- Select the **New Policy** button, and enter the New Policy Name, following the Policy naming conventions. Do not select the Copy from ... tic box.
- At the Edit QoS Device Class List, click on Telesyn and then the **Select** button
- The QOS Traffic Policy form appears with its list of attributes. Since this is a new policy, only the two default rules appear. If they are highlighted, select **Remove** (under Ip Filter Rules), and the result is a policy with no rules. (If they are not highlighted, select a rule and select **Delete Rule**.) Refer to the following figure.



QOS Policy Maintenance

Target Device Classes: Telesyn

Device Class	Target	Supported	Description
Rapier	☐	false	Allied Telesyn Rapiers, AT-88xx, AT-87xx and AT-86xx models
SwitchBlade	☐	false	Allied Telesyn SwitchBlade 4004, 4008 and AT-98xx models
Telesyn	☑	true	Telesyn 7000, and 9000 series Multi-Access Platforms
AT8900	☐	false	Allied Telesyn AT-89xx, AT-99xx, AT-99xxs and x900 models
ATRouter	☐	false	Allied Telesyn AT-AR400 Series and AT-AR750 routers

Policy Name: fx20queues

Description:

Policy Action: [Default Action]

Policy Rules

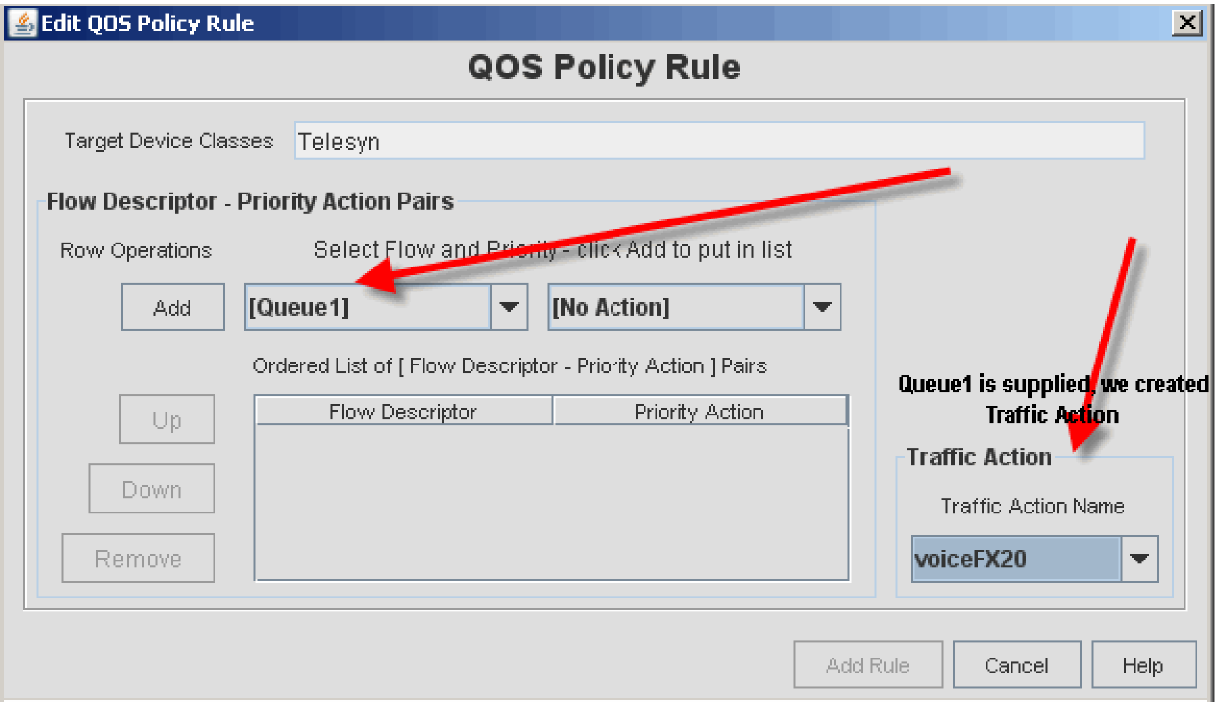
#	Flow	Priority	Traffic	Target Support
1	[IpFilterFlow]	[Allow]	[No Traffic Conditioning]	
2	[AnyOtherIp]	[Deny]	[No Traffic Conditioning]	

use Remove button to start from scratch

FIGURE 10-21 Creating a Policy with no Rules

3. Add the rules that will make up this policy.

- Select **Add Rule** under Row Operations.
- On the QOS Policy Rule Form, select the Flow as one of the pre-defined queue selections, and Traffic Action as one of the Actions that you created in Step 1. Refer to the following figure.



Edit QOS Policy Rule

QOS Policy Rule

Target Device Classes: Telesyn

Flow Descriptor - Priority Action Pairs

Select Flow and Priority - click Add to put in list: [Queue1] [No Action]

Ordered List of [Flow Descriptor - Priority Action] Pairs

Flow Descriptor	Priority Action

Queue1 is supplied, we created Traffic Action

Traffic Action

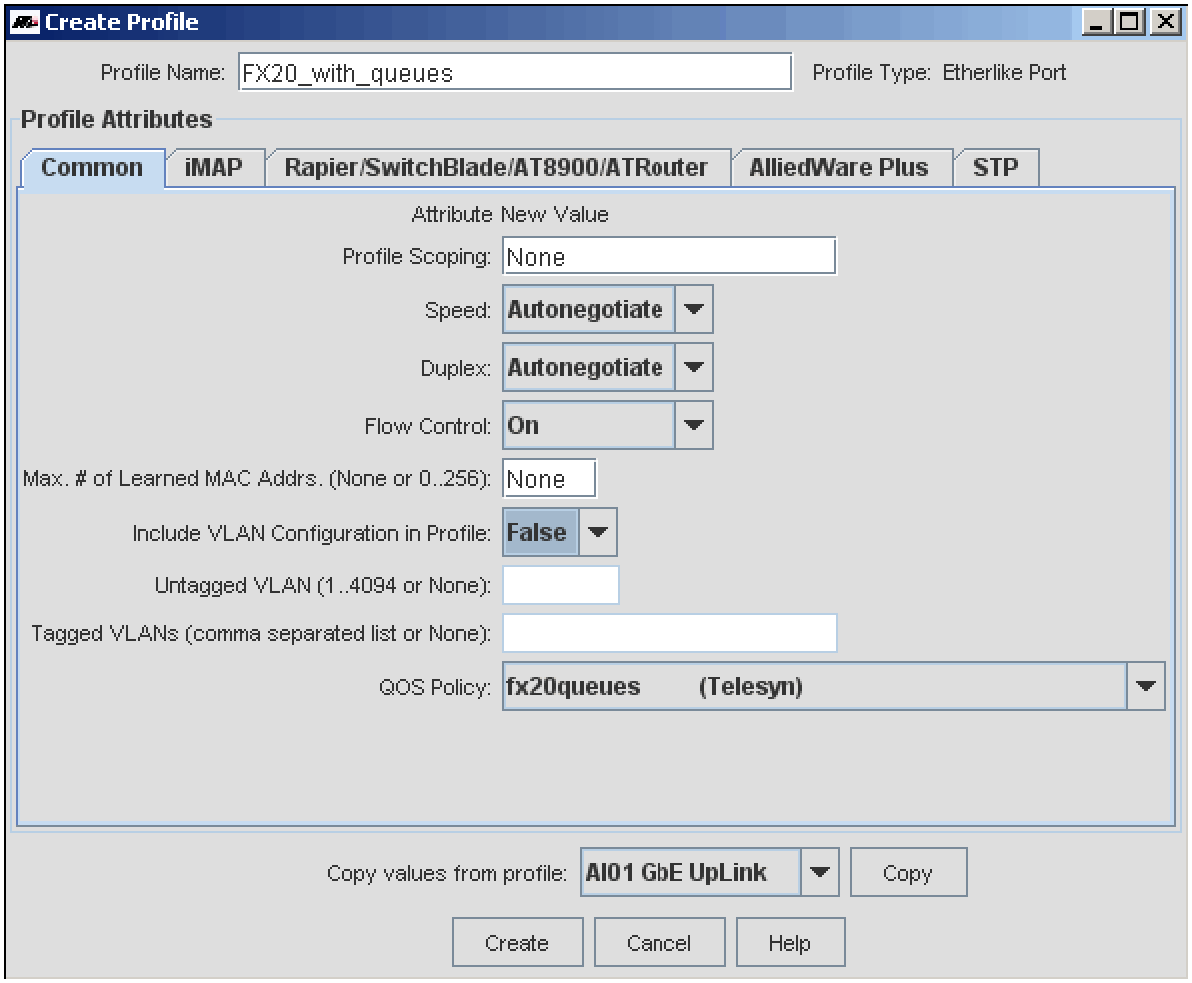
Traffic Action Name: voiceFX20

FIGURE 10-22 Creating a Rule for an FX20 Egress Queue

- Click on **Add**, and then **Add Rule** (there is no need to add multiple Flow Descriptor - Priority Action Pairs)
- The Rule is added to the Policy. Click on Add Rule and repeat these steps if there are additional rules.

4. With all of the rules created, click on **Save Policy**. The QosPolicy should be similar to Figure 10-19.
5. The QoSPolicy can now be incorporated into an Ether-like port profile. Refer to the following figure.

Caution: The Profile should be given a descriptive name, such as in the figure, to help ensure that this Profile is not included on a Triple_play provisioning form for ethernet ports other than the FX20.



Create Profile

Profile Name: FX20_with_queues

Profile Type: Etherlike Port

Profile Attributes

Attribute New Value

Profile Scoping: None

Speed: Autonegotiate

Duplex: Autonegotiate

Flow Control: On

Max. # of Learned MAC Addrs. (None or 0..256): None

Include VLAN Configuration in Profile: False

Untagged VLAN (1..4094 or None):

Tagged VLANs (comma separated list or None):

QOS Policy: fx20queues (Telesyn)

Copy values from profile: AI01 GbE UpLink

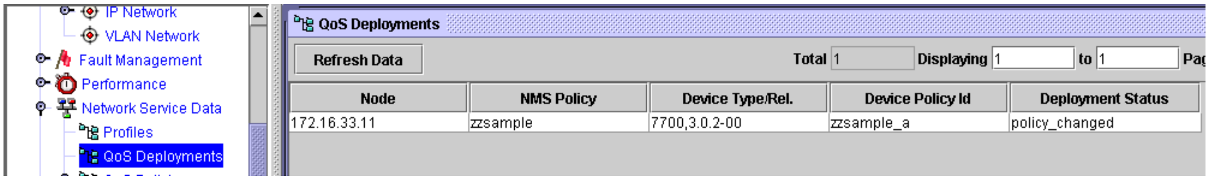
FIGURE 10-23 QOS Policy Included with an Etherlike Port Profile

11. Troubleshooting Policies and Profile Management

11.1 QoS Deployments Table

Since QoS Deployment has interrelationships with profiles and ports, there are some help procedures to understand these relationships and to use them to troubleshoot problems that may occur.

To view the status of policies, there is the QoS Deployments table, which lists the attributes of the policies and their deployment status. To access this table select **Network Services Data > QoS Deployments**, as shown in the following figure.



Total 1 Displaying 1 to 1

Node	NMS Policy	Device Type/Rel.	Device Policy Id	Deployment Status
172.16.33.11	zzsample	7700,3.0.2-00	zzsample_a	policy_changed

FIGURE 11-1 QoS Deployment Status

This table is used in many of the procedures below.

11.2 Determine which QoS Policy is Assigned to a Port

1. Locate the port in the *Network Inventory -> Ports table*.

2. The “Profile” column will indicate which NMS Profile is assigned to the port.

3. If the Profile Name has a “*” after it, then the NMS Profile is out-of-sync with the deployed port parameters. It should be redeployed to the port so that the port is in-sync with the Profile configuration.

4. Once the NMS Profile is in-sync, locate the Profile in the *Network Services -> Profiles* table and right-click on the Profile and select the **View Profile** item.

5. The “QOS Policy” parameter will show the name of the QoS Policy that has been assigned to the port.

11.3 Determine Whether a QoS Policy is Deployed and In-sync on a Device

1. Locate the Node (i.e. device) and NMS Policy in the *Network Services Data -> QoS Deployments* table.

2. If there is **not** a row for this in the table, then the QoS Policy has not yet been deployed to the device. If so, go to the *Network Services Data -> Profiles* table, select/create a Profile that assigns the desired QoS Policy and right-click to deploy the profile to the desired device.

3. If there **is** a row in the QoS Deployments table associated with the Policy and device, then verify that the QoS Policy deployment is in-sync with the QoS components on the device. This is reflected in the Deployment Status column. The status should show “no_changes”.

4. To re-check that the device policy has not been recently removed, right-click on the deployment row and select **Update Deployment Status**. This will cause the NMS to go to the device and verify that the policy is still there.

Caution: QoS components on the device that are associated with an NMS policy should not be edited via CLI. These changes may not be detected by the NMS, in which case the status will continue to show “no_changes”. For efficiency reasons, the NMS will *not attempt to re-deploy policies that are determined to be in-sync. As a result, if underlying CLI QoS component changes are suspected, you must force the NMS to redeploy the NMS policy.*

To **redeploy** the NMS policy can be done in one of several ways:

- If the redeployment is only required on a single device, then right-click on the desired row of the QoS Deployment table and select **Undeploy Policy**. This will remove the corrupt QoS components from the device. At this point redeploying the port Profile will automatically update the QoS Policy on the device.
- If, on the other hand, you would like to update the QoS Policy on all devices, the simplest way to force the NMS to redeploy the policy is to modify the QoS Policy definition and resave it. This will cause all deployments of that policy to be flagged with a status of "policy_changed", which will force all policies to be redeployed on the next Profile deployment.

After the **Update Deployment Status** operation is performed, if the Deployment Status indicates a policy or device change has been detected, then this may be the source of the problem. If so, go to the *Network Services Data -> Profiles* table, select the associated Profile that assigns the desired QoS Policy and right-click to redeploy the profile to all of its assigned ports. This will bring the devices back in-sync with the NMS Policy.

11.4 Determine whether a QoS Policy has the Desired Configuration

1. Locate the desired QoS Policy in the *Network Services Data -> QoS Policies* table, and right-click on it, selecting the **View/ Edit Policy** item. This will bring up the details of the Policy.

2. Confirm that the Policy Rules appear as intended. You can select the **Show Errors** button to re-check for any obvious errors.

3. Analyze the Flow, Priority, and Traffic Descriptor definitions, by selecting their respective buttons at the bottom of the window. Browse through the definitions associated with the policy.

4. Review the Flows and identify any rules with intersecting flows. Different devices/interfaces handle multi-rule matches differently. Some interfaces will perform the actions only on the first rule to be matched by the incoming packet, while others will perform actions from multiple matching rules, provided the actions do not conflict with each other.

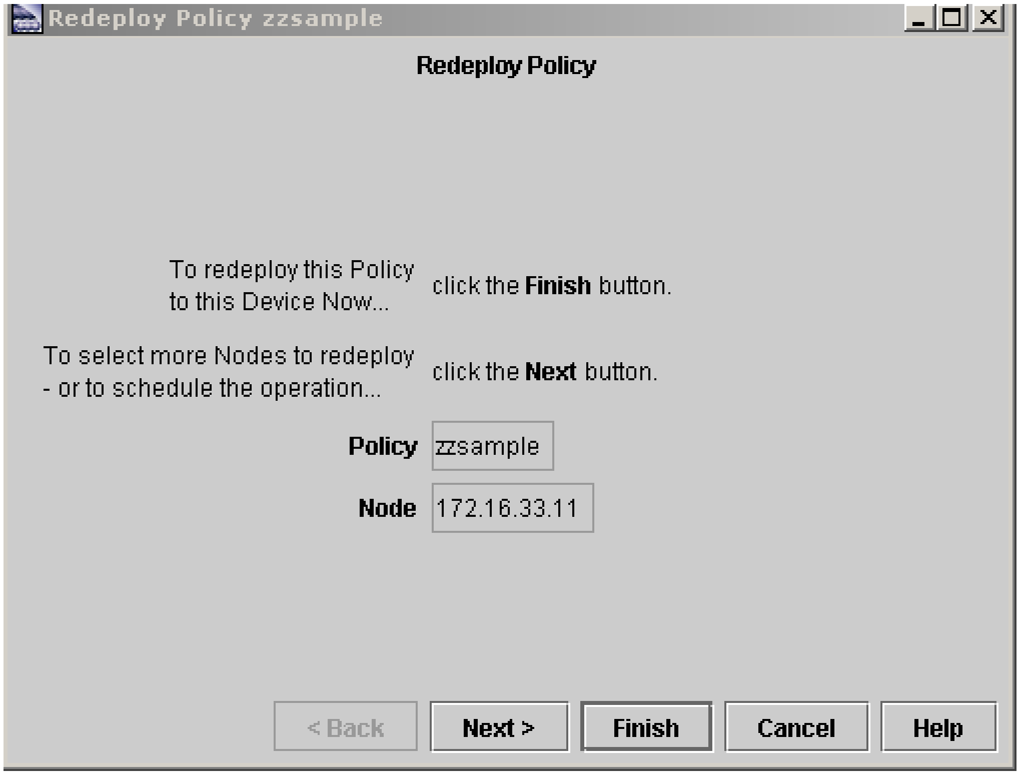
Note: Please see the device specific details for handling intersecting rules.

5. If a configuration problem is discovered, modify the QoS Policy (including any flow or action descriptors that need to be changed) to correct the problem, then save and close the window. This will flag all affected QoS Deployments to have a Deployment Status of "policy_changed".

Since Flows and Actions may be shared among multiple QoS Policies, you may find that changes to them will affect other policies as well. These will also be reflected in the status entries of the QoS Deployments table, as explained in the next subsection.

11.5 Redeploying Policies

To redeploy a policy for a device or set of devices, right-click on a row of the deployment table and select **Redeploy Policy**. Refer to the following figure.



Redeploy Policy zzsample

Redeploy Policy

To redeploy this Policy to this Device Now... click the **Finish** button.

To select more Nodes to redeploy - or to schedule the operation... click the **Next** button.

Policy zzsample

Node 172.16.33.11

FIGURE 11-2 Redeploy Policy

Clicking on Finish at this point will redeploy the policy for that device. Clicking on **Next** brings up the Select Deployments form. This allows the user to redeploy a policy to the set of devices that have the policy deployed and to schedule the redeployment. Refer to the following figure.

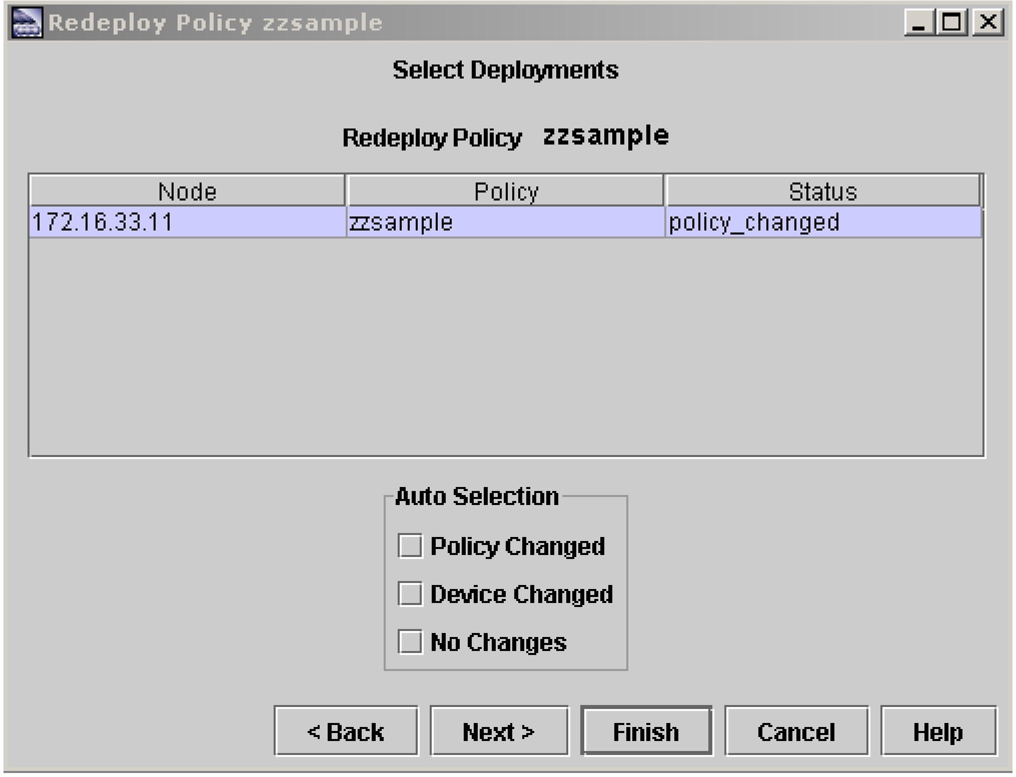
The table includes all the devices that have the policy. One column, Status, is the relationship between the policy and the device:

- Policy Changed - The policy has changed, but the device policy does not match.
- Device Changed - The policy on the device has changed, but the policy has not changed.
- No changes - As far as what has been configured, there have been no changes.

The Auto Selection panel can be used to redeploy the policy to all the devices (by not checking any tic boxes) or selecting only those devices that are in these states (checking the tic boxes).

Selecting **Finish** starts the task immediately, while selecting Next will allow the task to be added to a schedule.

Note: In most situations, redeploying a policy is done more efficiently by changing the policy and redeploying the profiles that use that policy.



Select Deployments

Redeploy Policy zzsample

Node	Policy	Status
172.16.33.11	zzsample	policy_changed

Auto Selection

□ Policy Changed

□ Device Changed

□ No Changes

FIGURE 11-3 Select Deployments

6. For multiple devices, and to update port parameters as well, locate the affected port profiles and use the profiles table to redeploy to all affected devices.

12. Controlling and Provisioning Network Devices

You can provision a single device or a set of devices together. Provisioning options include:

- Backup/Restore
- Command Script Management
- Configuration File Management
- Device Information
- Syslog Management
- SNMP Agent
- SNMP Community
- SNMPv3 USM Configuration
- Software Configuration
- LLDP Configuration
- Configure VLAN
- Card Management
- Port Management

When multiple devices are selected, only those operations that can be performed on more than one device are active.

The following subsections go through all of the menu options available for the AT Network Elements. Separate subsections highlight the provisioning tasks.

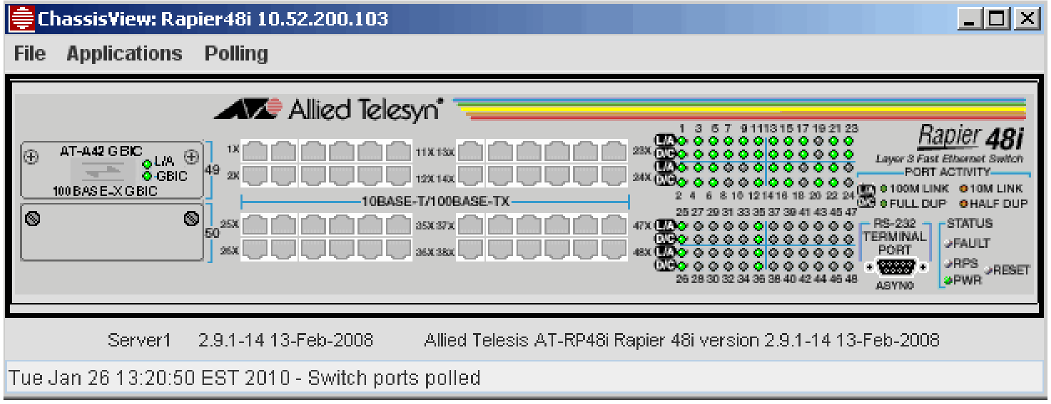
Use the following table to locate the task you wish to perform.

The NMS supports all cards that can be configured with the various CFC cards, and this is reflected in the chassis view as well as the various types of management. Refer to the *iMAP Component Specification* for the available CFC cards and the products they support.

12.1 View Chassis

To view the connection layout of a device:

- Right-click on the device and select **View Chassis**. An image of the product appears.



Server1 2.9.1-14 13-Feb-2008 Allied Telesis AT-RP48i Rapier 48i version 2.9.1-14 13-Feb-2008

Tue Jan 26 13:20:50 EST 2010 - Switch ports polled

FIGURE 12-1 Chassis view of a Rapier Product

For Rapier products, the chassis image shows in real-time the status of the links and ports. The link LEDs indicate the link state for each port. A legend on the chassis face interprets the meaning for the LED colors, such as green for an enabled 100 MHz link and amber for an enabled 10 MHz link.

The port status is indicated on the chassis face by the port color. During normal operation, the port color is gray. If an alarm occurs on a port, the color of the affected port will change to indicate the alarm condition. When the alarm is cleared, the port color will change back to gray. If multiple alarms exist, the highest priority alarm condition will be displayed. When the highest-priority alarm condition is cleared, the next lower priority alarm will be displayed.

The File pull-down has the **Refresh** and **Exit** options, while the **Applications** pull-down has the **VLAN Interface Configuration** option. This will invoke the VLAN view of the device and allow for VLAN provisioning, as described in "Configure VLAN (Chassis View)" on page 335.

Note: The Refresh option is useful in picking up any card configuration changes.

The **Polling** pull-down is a toggle function to Start or Stop Port Pollers; the pollers allows port information to be polled for the device so the port status can be updated. Along the bottom of the Chassis View is the date when the switch ports were last polled.

Below the device is general information about the device.

For iMAP products, the chassis view reflects which cards are configured and in what slot they are located. A graphical representation of each provisioned card is displayed, including the colors of any LEDs and any markings on the card face. An example is shown in the following figure.

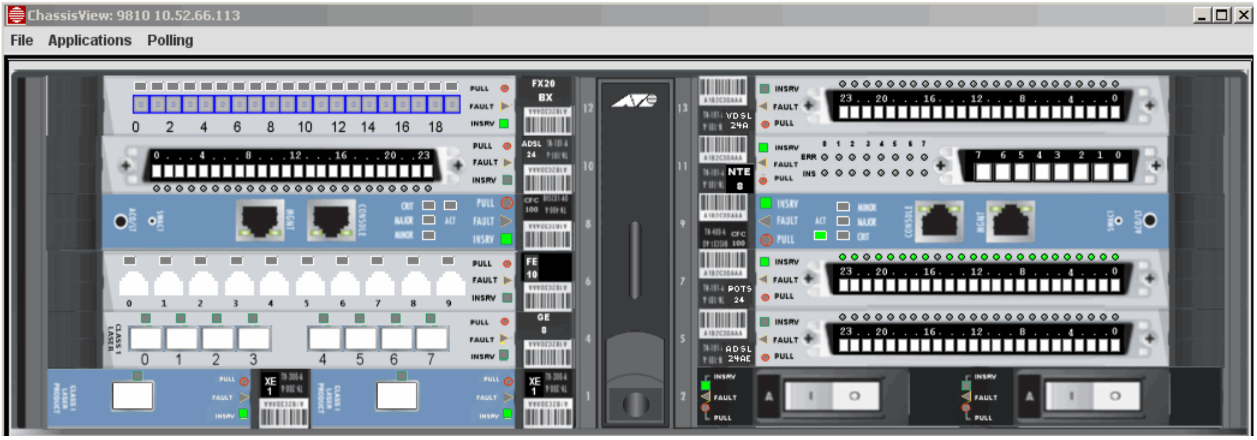


FIGURE 12-2 Chassis view of a iMAP Product (9810)

For iMAP devices, alarm LEDs for the chassis view are known by polling the device for alarms, not by querying the AlliedView NMS database that has the results of the AlliedView NMS Management system (described in Section 8). Therefore, alarm LEDs produced as a result of the Fault Management system (such as thresholds or traps) are not are known by the chassis view and are not displayed.

For the EPON2 card, the port LED is lit when there is a discovered link on the EPON interface. (The link does not have to be authenticated.). Also for the EPON2 card, you can click on the ONU button and a pop-up will show the status of the ONU ports. To close the pop-up, click on the square labeled Port <no.> ONUs, as highlighted in Figure 12-2.

12.1.1 Display Types

There are four types of displays for cards in the chassis view:

- Card is provisioned and installed - The card is displayed.
- Card is pre-provisioned but not installed - The card appears as a provisioned/installed card, but the LEDs indicate the *provisioned* card state, and the Fault LED is lit with the “card not present” fault.
- Card is installed but not provisioned - The card appears grayed-out and has the label “NOT PROVISIONED” across the front as shown in the following figure.

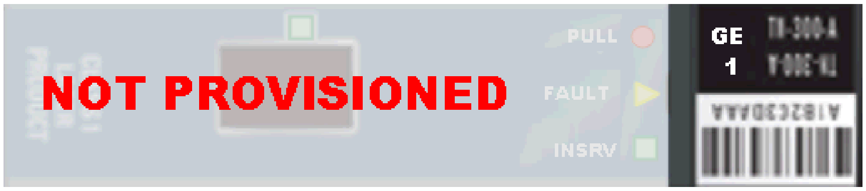
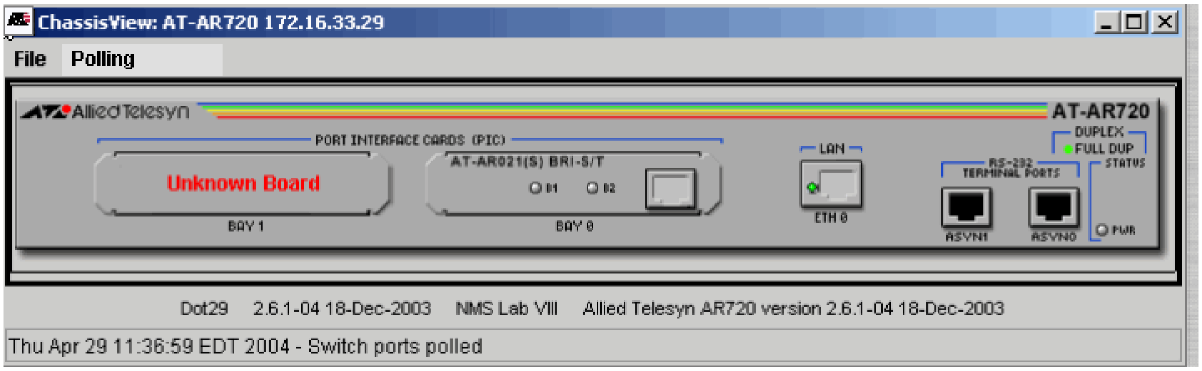


FIGURE 12-3 An Example NOT PROVISIONED Card in the Chassis View

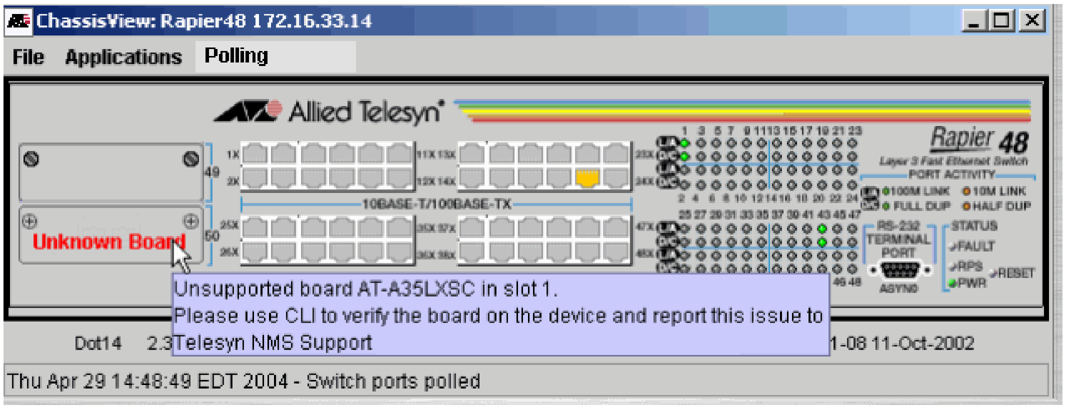
- Unknown card - When the chassis view detects a card that is not supported, it displays the board with an “Unknown Board” image. Refer to the following figure.



Dot29 2.6.1-04 18-Dec-2003 NMS Lab VIII Allied Telesyn AR720 version 2.6.1-04 18-Dec-2003

Thu Apr 29 11:36:59 EDT 2004 - Switch ports polled

FIGURE 12-4 An UKNOWN Card in the Chassis View - AT-AR720 Device



Unsupported board AT-A35LXSC in slot 1.
Please use CLI to verify the board on the device and report this issue to Telesyn NMS Support

Dot14 2.3 1-08 11-Oct-2002

Thu Apr 29 14:48:49 EDT 2004 - Switch ports polled

FIGURE 12-5 Tooltip for an Unknown Board Image

Like the Rapier product chassis view, this view also has the **Refresh** and **Exit** options, while the **Applications** pull-down has the **VLAN Interface Configuration** option.

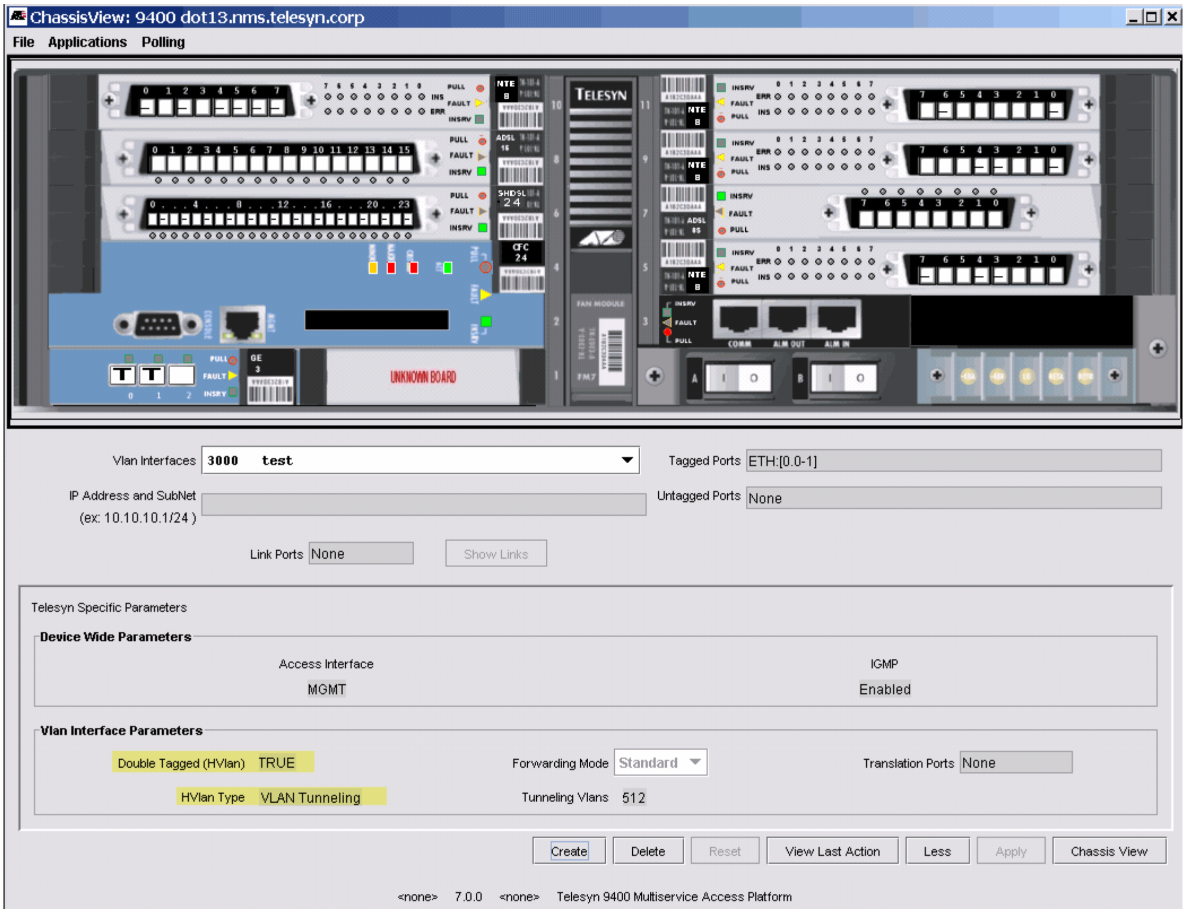
The **Polling** pull-down is a toggle function to Start or Stop Poll Pollers; the pollers allows port information to be polled for the device so the port status can be updated. Along the bottom of the Chassis View is the date/time when the switch ports, card states, and alarms were last polled. As each is updated, each will replace the previous poll result.

Note: Polling is suspended while Vlan data is retrieved or updated.

Note: For the AT-x610, stacking will not start until after the unit has been booted and the stack-XG card has already been inserted. If the card is removed (or is replaced), and the x610 is not rebooted, the chassis view shows a duplicate image.

12.1.2 Display of VLAN-based HVLANs (Tunneling)

For the iMAP and SBx3100, an outer tag can be applied for certain ethernet-based cards, allowing an outer VLAN to be applied to several customer interfaces. The NMS cannot be used to create these, but the chassis view does show where these tunneling-type HVLANs are located. Refer to the following figure.



Vlan Interfaces: 3000 test

Tagged Ports: ETH:[0.0-1]

IP Address and SubNet (ex: 10.10.10.1/24)

Untagged Ports: None

Link Ports: None

Telesyn Specific Parameters

Device Wide Parameters

Access Interface: MGMT

IGMP: Enabled

Vlan Interface Parameters

Double Tagged (HVlan): TRUE

Forwarding Mode: Standard

Translation Ports: None

HVlan Type: VLAN Tunneling

Tunneling Vlans: 512

<none> 7.0.0 <none> Telesyn 9400 Multiservice Access Platform

FIGURE 12-6 Tunneling VLANs Displayed on Chassis View

12.1.3 Notes on Chassis View

Following are device-specific notes on the chassis view:

- 9000 devices
  - Displaying port status/alarms in the Chassis View is supported.
  - Filler plates are included in the chassis view.
  - Support the FAN8 module in the 9700. This module is always displayed (even if removed for maintenance). The states of the Pull, Fault and Insrv LED components on the Fan module in Chassis View reflect those of the LEDs on the physical device.
  - The “Pull” LED appears gray for a pre-provisioned (i.e. not present) board.
  - When the mouse is over a card, a tool tip indicates the Status (Online, Not Installed etc) of that card.
  - The “Unknown Board” image for the iMAP devices now represents either a board which is not supported by the NMS, or a board which is not recognized by the device.
  - A pre-provisioned card in the Chassis View is distinguishable from a physically present card by the following visual cues.

    - The yellow “fault” LED is lit and the associated fault is “Card Not Present” viewable by moving the mouse over the LED image.

    - The “Pull” and “Insrv” LEDs are gray. In a physical card, one or the other of these will be on at all times.

    - The status of the card is “Not Installed”, viewable by moving the mouse over the card background.
- AT-8324
  - The Chassis View for the AT-8324 shows the chassis as a module; if multiple AT-8324s are stacked then they will all be displayed in one dialog, as a stack.
  - The following uplink boards are supported in Chassis View:, AT-A15/LX, AT-A15/SX, AT-A16, AT-A17, AT-A17/SM15, AT-A18, AT-A19.
  - Fault LED on the main chassis is not monitored.
  - The “master” LED on the main chassis is not monitored.
  - Displaying port alarms in the Chassis View is currently not supported.
- AT-AR7xx
  - The 4 ports on the AR026 board are pure switch ports. They multiplex into one internal ETH port. The Link LED displayed on the AR026 in Chassis View, shows the operational state of the internal port. Since these switch ports do not map to individual interfaces, they cannot be managed by the NMS.

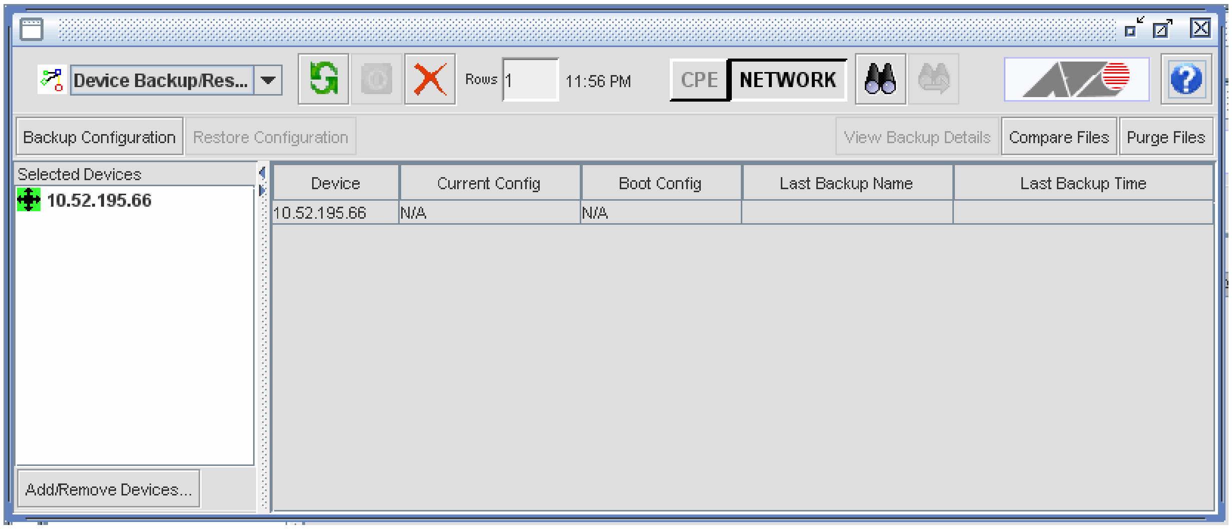
12.2 Provisioning a Device

12.2.1 Overview of the Provisioning Interface

When selecting a device or set of devices for an application, you must choose the application as well as the specific devices that are to share that application. This section describes an example walkthrough of how to select the set of devices.

When selecting the provisioning option, you must first select one of the applications. The following figure shows what appears after right clicking on the device and selecting *Provision - > Backup/Restore*

Note: *When using the provisioning feature, the AlliedView NMS is aware of how many devices have been selected for each application. When you go from one application to another, the original application remains with its set of devices and state: if you return to the first application, it retains that status and set of devices.*



Device	Current Config	Boot Config	Last Backup Name	Last Backup Time
10.52.195.66	N/A	N/A		

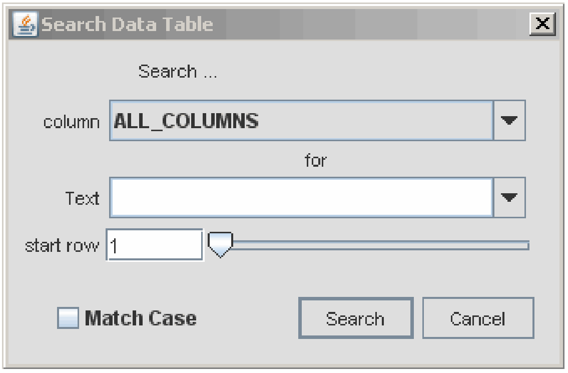
FIGURE 12-7 Selecting a Device for Backup/Restore

The selected device is included in the Selected Devices column. The following table describes the buttons that are available once an application is selected.

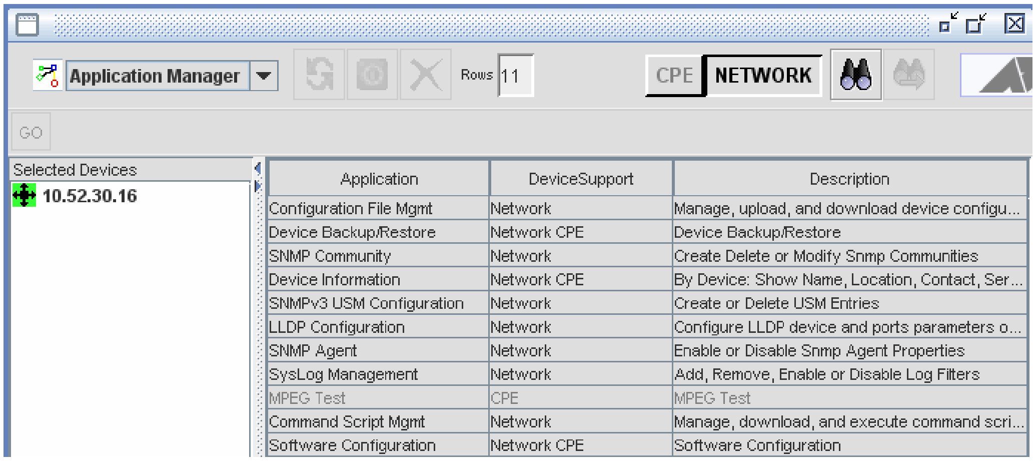
TABLE 12-1 Buttons Common to Applications

Button Icon	Meaning	Description
🔄	Collect Data	Gathers data from all the devices for the application
⊘	Abort	While data is being collected, this stop sign icon is red. Clicking on the icon at that point will stop the data collection.
✕	Delete all	Deletes all collected data in the generated table
Rows 5	Rows	Number of rows currently in the table
Time in 24-hour format (next to Rows)	Collection Time	Once an application is run, the date and/or the time it was run
CPE NETWORK	CPE versus Network Device	Toggles between the Allied Telesis Network Devices (iMAP, Rapier, AT) and iMG/RG devices.

TABLE 12-1 Buttons Common to Applications (Continued)

Button Icon	Meaning	Description
	Search	Brings up search dialog allowing search by column for a text string, with options for starting row and matching cases shown here:  Search Data Table Search ... column ALL_COLUMNS for Text start row 1 ☐ Match Case Search Cancel Table cells with the text are highlighted yellow.
	Search Next	Once a text string is found, find the next table cell that has the text string.
	Allied Telesis Logo	This button is enabled when a task is started but not complete, and animated while the data collection or the application task is active. Note that scheduled tasks run independently and so do not activate this button. However, any values that are being updated in the displayed application table will be updated.
?	Help	Invokes context-sensitive help

At this point, you would normally click **Add/Remove Devices** at the bottom of the window and create a set of devices to include in the application. You can also go to the pull-down menus and select **Application Manager**, which lists all the applications available for the device, as shown in the following figure.



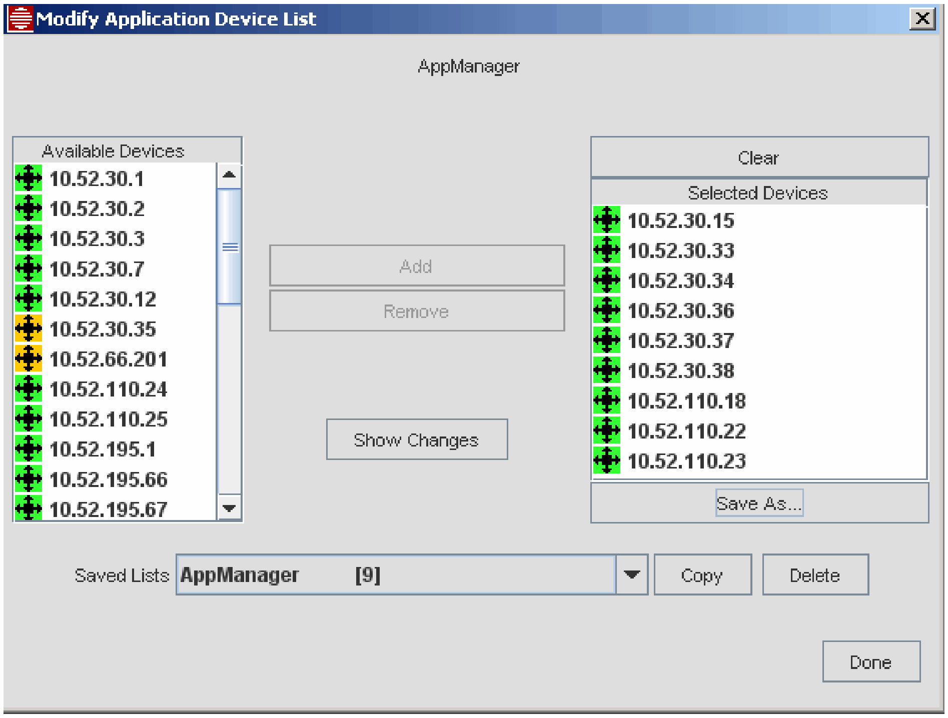
Selected Devices
10.52.30.16

Application	DeviceSupport	Description
Configuration File Mgmt	Network	Manage, upload, and download device configu...
Device Backup/Restore	Network CPE	Device Backup/Restore
SNMP Community	Network	Create Delete or Modify Snmp Communities
Device Information	Network CPE	By Device: Show Name, Location, Contact, Ser...
SNMPv3 USM Configuration	Network	Create or Delete USM Entries
LLDP Configuration	Network	Configure LLDP device and ports parameters o...
SNMP Agent	Network	Enable or Disable Snmp Agent Properties
SysLog Management	Network	Add, Remove, Enable or Disable Log Filters
MPEG Test	CPE	MPEG Test
Command Script Mgmt	Network	Manage, download, and execute command scri...
Software Configuration	Network CPE	Software Configuration

FIGURE 12-8 Selecting the Application Manager to View all Applications

Many of the buttons are grayed out because an application has not been selected. At this point, the user can double-click on one of the Applications in the table (or select the application, and then click **GO**) and it will invoke the specific application window.

If the user clicks **Add/Remove Devices**, which is at the bottom of every application window, the set of devices that are to be included in the application can be controlled, as shown in Figure 12-9.



Available Devices
10.52.30.1
10.52.30.2
10.52.30.3
10.52.30.7
10.52.30.12
10.52.30.35
10.52.66.201
10.52.110.24
10.52.110.25
10.52.195.1
10.52.195.66
10.52.195.67

Selected Devices
10.52.30.15
10.52.30.33
10.52.30.34
10.52.30.36
10.52.30.37
10.52.30.38
10.52.110.18
10.52.110.22
10.52.110.23

Saved Lists: AppManager [9]

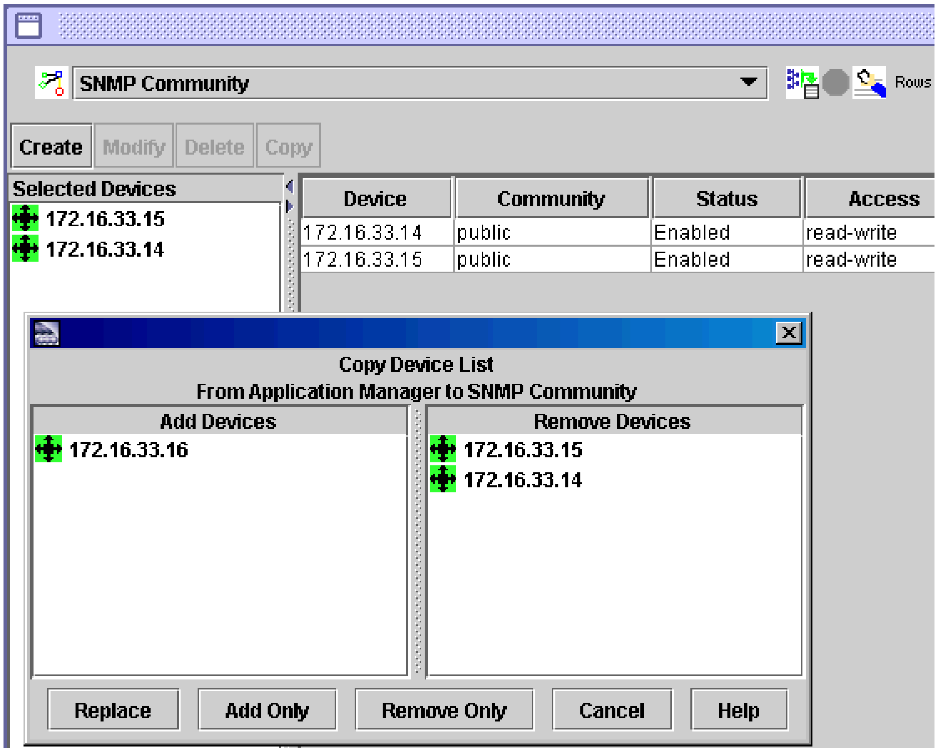
FIGURE 12-9 Add / Remove Devices for an Application

Table 12-2 lists the options for the **AppManager** window. Click **Done** to close the window.

TABLE 12-2 Options for the Add / Remove Devices for an Application

Option	Description
Available Devices	Available devices for the application are in black.
Clear	Clear all devices from the **Selected Devices** list.
Add / Remove	Sends a device from one column to another.
Show Changes	Brings up a window that shows which devices were added or removed from when the window was first invoked.
Save As...	Saves the currently displayed **Selected Devices** list to be recalled at a later time.
Saved Lists	Is a drop-down list of saved lists created with the **Save As** button. Selecting a saved list and then clicking **Copy** will copy the devices in the saved list to the **Selected Devices** panel. The number of devices in each list is indicated in square brackets to the right of the list name. The saved list also contains the list for each application so they can be copied to other applications.
Copy	Copies the devices in a saved list to the **Selected Devices** panel.
Delete	Delete the selected Saved List
Done	Makes the changes and puts the devices in the application window.

Another option to control the set of devices to be included in an application occurs when moving from one application (or the AppManager) to another, and the target Applications List is different (but not empty) from the source Applications List. The **Copy Device List** window appears, as shown in Figure 12-10.



Selected Devices
172.16.33.15
172.16.33.14

Device	Community	Status	Access
172.16.33.14	public	Enabled	read-write
172.16.33.15	public	Enabled	read-write

Copy Device List
From Application Manager to SNMP Community

Add Devices
172.16.33.16

Remove Devices
172.16.33.15
172.16.33.14

FIGURE 12-10 Copy Device List for an Application - File

The example shown in Figure 12-10 would occur if you have previously collected data for devices 172.16.33.14 and 172.16.33.15, and then right-click device 172.16.33.16 for the SNMP Community application. The Application window appears showing the devices that have already had data collected, and the **Copy Device List** also appears with the following options:

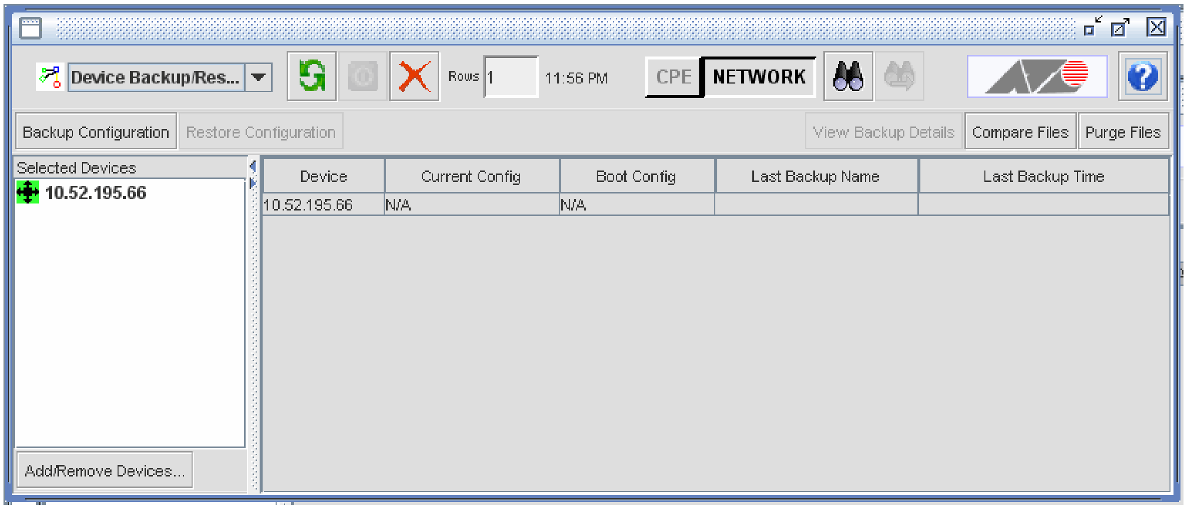
- **Replace** - Replace the target application device list with the source application device list. In this case, the 172.16.33.14 and .15 devices are replaced with the .16 as a Selected Device.
- **Add Only** - Add the .16 device to the other two devices.
- **Remove Only** - Remove devices from the target list that are not in the source list. In this case, the .14 and .15 devices would be removed.

12.2.2 Backup/Restore (with Purge Button)

The *Device Backup/Restore* option creates a current configuration data backup file for each managed device.

Note: *Devices selected that are not supported will not appear in the Selected Devices list when the Device Backup/Restore application is selected.*

The user can add or remove devices to the list of selected devices, as explained in "Overview of the Provisioning Interface" on page 275. Once all of devices for the device backup restore are in the Selected Devices column, click the **Collect Data** icon. The AlliedView NMS begins gathering data, the **Stop** icon is highlighted, and as the data is collected they are added to the device table, as shown in the following figure.



Rows 1

Selected Devices
10.52.195.66

Device	Current Config	Boot Config	Last Backup Name	Last Backup Time
10.52.195.66	N/A	N/A		

FIGURE 12-11 Collected Data for Selected Devices for Device Backup Restore (Network Selected)

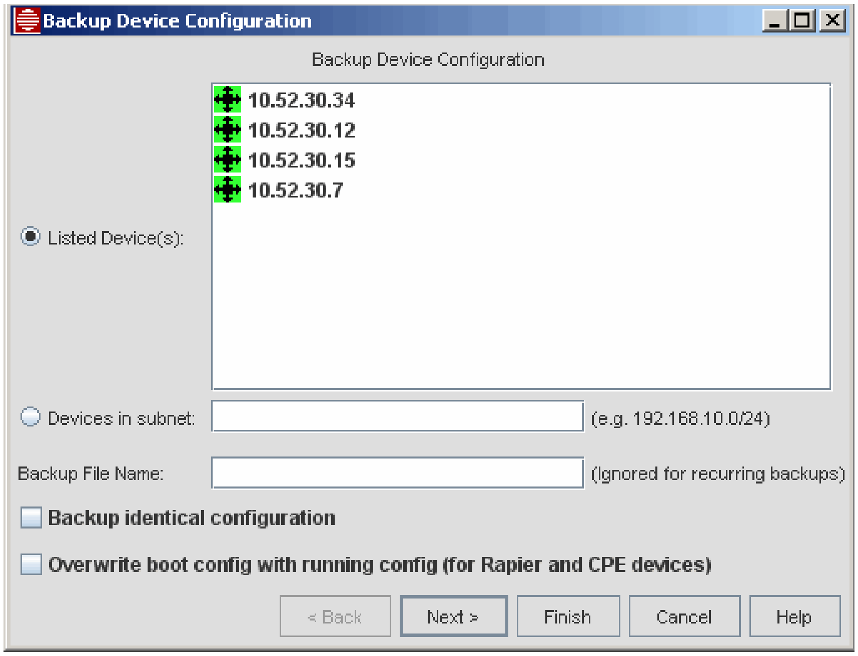
Note: *If for any devices the data cannot be collected, the row is dark; the Tooltip for that row will include the reason, such as "Unable to Connect."*

12.2.2.1 Performing Backups

At this point the user can perform the following:

- Select multiple devices and perform a backup only.
- Select one device and perform a backup or restore.

Figure 12-12 shows the initial backup window, while Table 12-3 describes the fields.



Backup Device Configuration

● Listed Device(s):
10.52.30.34
10.52.30.12
10.52.30.15
10.52.30.7

○ Devices in subnet: (e.g. 192.168.10.0/24)

Backup File Name: (Ignored for recurring backups)

□ Backup identical configuration

□ Overwrite boot config with running config (for Rapier and CPE devices)

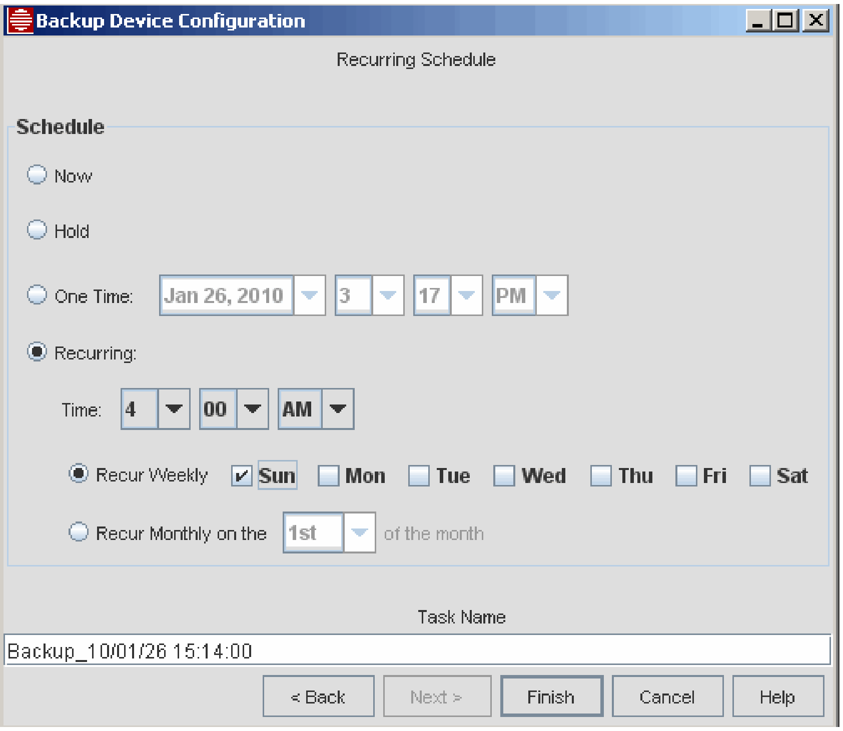
FIGURE 12-12 Initial Backup Window

TABLE 12-3 Backup Device Configuration Fields

Field	Meaning
Listed Device(s)	Device(s) that will have a backup created.
Devices in subnet	Backs up all devices for the specified subnet. The query is done when the task is executed, so that for a recurring task, new devices added since that task was created will be backed up during the next execution of the task.
Backup File Name	Descriptive name for the backup file. If the filename is not specified, the filename is generated by the NMS and will include the date and time of the backup.
Backup identical configuration	When checked, backs up and saves configuration files for devices where the files have not changed. The default is not to save identical configuration files (the tic box is not checked).
Overwrite boot config with running config (for Rapier and CPE devices)	Make the current configuration (reflected in the configuration database) the default. This applies to Rapier and CPE devices only.

Note: If you have modified your network configuration for Rapier or CPE devices, such as adding or modifying VLANs, you should back up your configuration information as soon as possible. Make sure the Overwrite boot configuration file with running configuration checkbox is checked.

If the backup is to occur now, click **Finish**. For scheduled or Recurring backups, click **Next**, and the **Recurring Schedule** window will appear, as shown in the following figure.



Backup Device Configuration

Recurring Schedule

Schedule

○ Now

○ Hold

○ One Time: Jan 26, 2010 3 17 PM

● Recurring:

Time: 4 00 AM

● Recur Weekly ☑ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

○ Recur Monthly on the 1st of the month

Task Name

Backup_10/01/26 15:14:00

FIGURE 12-13 Recurring Backup Schedule Window - File

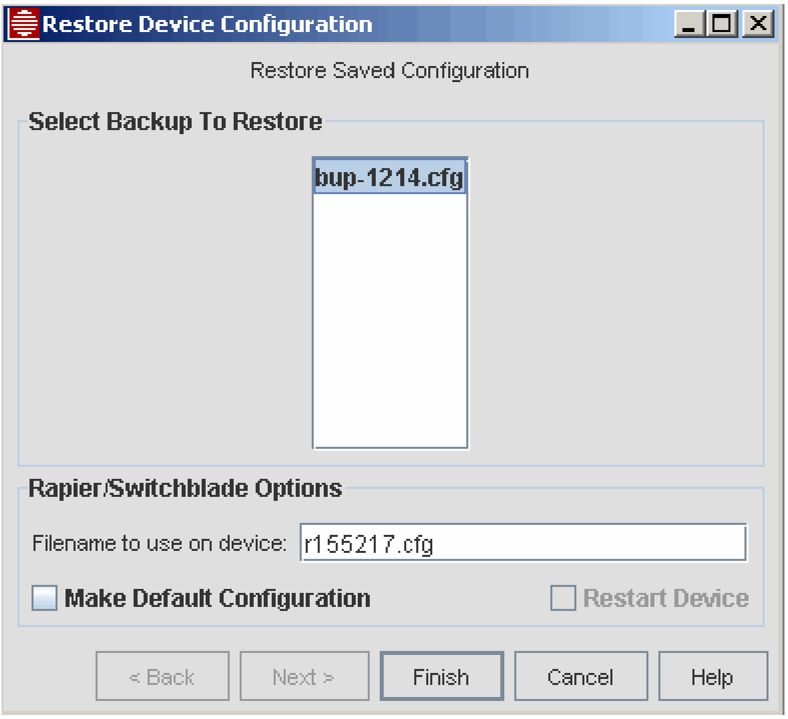
In Figure 12-13, the backup has been scheduled for Sunday morning at 4 a.m. every week. Clicking **Finish** adds the backup to the schedule.

Note: It is highly recommended that you configure your device configuration backup to run on a recurring schedule to preserve configuration changes made by the NMS. If a device reboot or, in the case of iMAP devices, a database purge occurs, any configuration data that is not backed up will be lost. With regularly scheduled backups, should such an event occur, you can restore your configuration changes from the backup files.

12.2.2.2 Restore Configuration (Options Depend on Device Type)

Once a device or set of devices has a backup file, it can be restored. Select a device that has a backup file and click **Restore Configuration**. One of the following figure appears, depending on the device to be restored.

For Rapier/Switchblade devices only, the Rapier/Switchblade options are enabled, as shown below.



Restore Device Configuration

Restore Saved Configuration

Select Backup To Restore

bup-1214.cfg

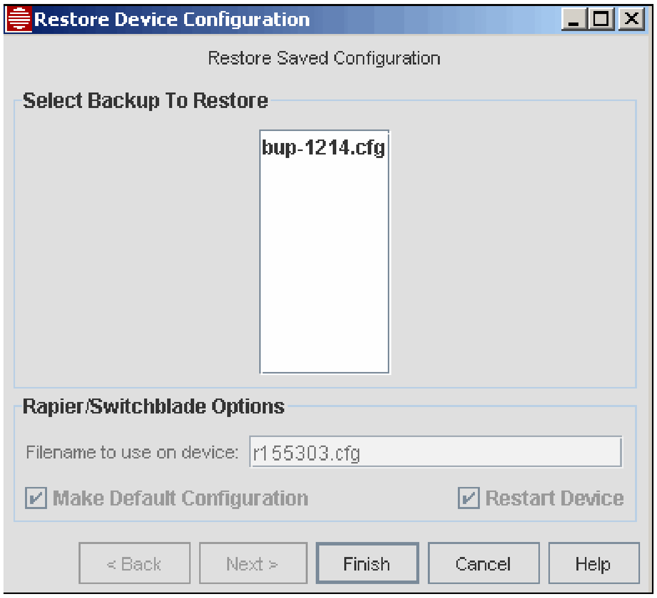
Rapier/Switchblade Options

Filename to use on device: r155217.cfg

☐ Make Default Configuration ☐ Restart Device

FIGURE 12-14 Restore Configuration for Rapier / SwitchBlade Devices Only

For iMAPs devices, the lower panel checkboxes are disabled, as shown below.



Restore Device Configuration

Restore Saved Configuration

Select Backup To Restore

bup-1214.cfg

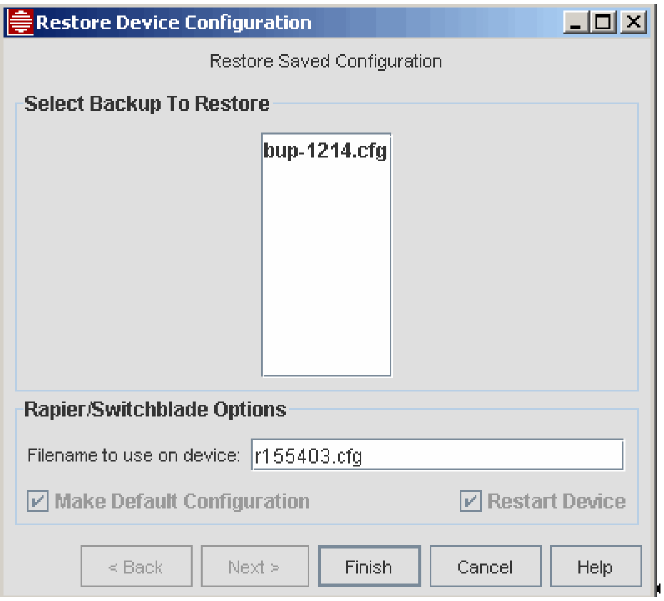
Rapier/Switchblade Options

Filename to use on device: r155303.cfg

☑ Make Default Configuration ☑ Restart Device

FIGURE 12-15 Restore Configuration for iMAP Devices Only

For iMAP and Rapier/Switchblade devices, the Rapier/Switchblade filename option is enabled but checkboxes are disabled, as shown below.



Restore Device Configuration

Restore Saved Configuration

Select Backup To Restore

bup-1214.cfg

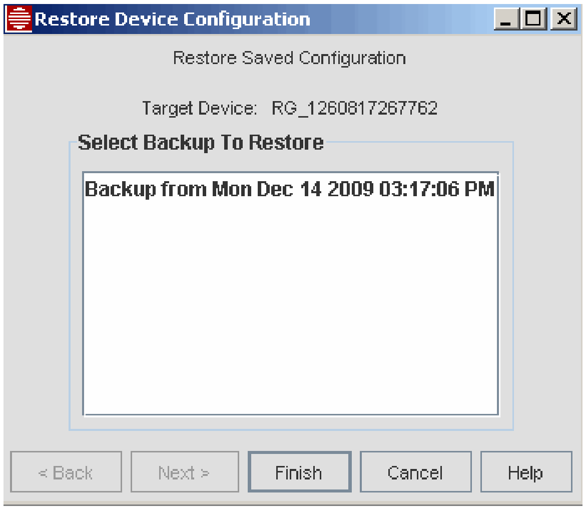
Rapier/Switchblade Options

Filename to use on device: r155403.cfg

☑ Make Default Configuration ☑ Restart Device

FIGURE 12-16 Restore Configuration for iMAP and Rapier / SwitchBlade Devices

For iMG/RGs only, these cannot be selected with iMAPs, Rapiers, etc, and the entire lower panel is removed, as shown below.



Restore Device Configuration

Restore Saved Configuration

Target Device: RG_1260817267762

Select Backup To Restore

Backup from Mon Dec 14 2009 03:17:06 PM

FIGURE 12-17 Restore Configuration for iMG/RG Devices

There is the option to make the restored file the default configuration. If this option is chosen, the **Restart Rapier** checkbox is active and can be used to restart the Rapier with the restored file.

The following table lists the options available.

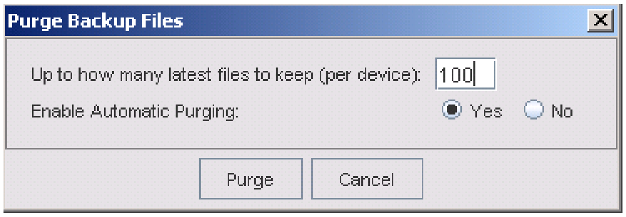
TABLE 12-4 Restore Device Configuration Fields

Option	Description
Backup File	A list of files from which you choose the one to send to the device.
Filename to Use on Rapier	This field is filled in as you select a backup file. If the user didn't specify a filename for the backup, the entry will be "Backup from <date time>. Applies to all devices except iMG/RG.
Make Default Configuration	Checkbox that makes the selected file the default file (when device restarts, it will use this file). For Rapier / SwitchBlade devices only.
Restart Device	If the Make Default Configuration checkbox is checked, the Rapier device will restart immediately with the default file when the Apply button is pressed.
Apply	Applies the Changes.
Close	Closes the window. If the Apply button was not pressed, the options will not take effect.

12.2.2.3 Use of the Purge Files Option

The Purge Files button is added to the Device Backup/Restore panel to provide a way to activate on-demand purging and to configure the backup limit parameter using the NMS client.

Selecting the Purge Files button pops up a "Purge Backup Files" dialog, from which the user can enter the number of files to keep and whether or not to enable automatic purging for future backups. Refer to the following figure.


Purge Backup Files

Up to how many latest files to keep (per device): 100

Enable Automatic Purging: ● Yes ○ No

FIGURE 12-18 Purge Backup Dialog

Note: *The value for what appears is from the AT_NmsBackupFiles.conf configuration file. The number must be greater than 0. Refer to "Device Backup (Per-Device Limit)" on page 131.*

The dialog includes a "Purge" button to activate purging and a "Cancel" button to dismiss the dialog without executing a purge.

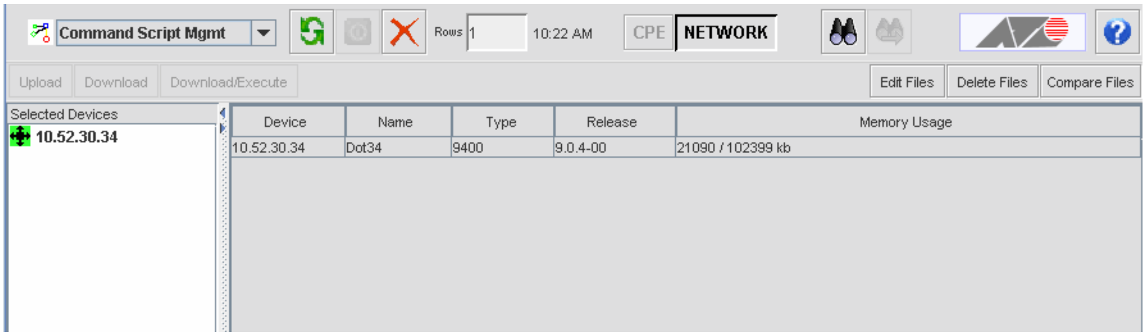
Selecting Purge brings up the confirmation dialog. If the user confirms the operation, then all but the latest number of files per device will be deleted. Also, the `AT_NmsBackupFiles.conf` configuration file will be updated if a different value was entered (for example other than the 100 shown in the figure).

12.2.3 Command Script Management

Scripts are user-defined command (CLI) files. With the **Command Script Mgmt** window, the user can retrieve script files from a device or from the AlliedView NMS server, edit them in a multi-paged editor, and execute them. Moreover, the scripts can be executed on multiple devices at once.

Note: *For Rapier devices, significant configuration changes made using command scripts will not be reflected in the NMS until the devices are rediscovered. (Rediscovery can occur automatically as configured in Discovery Configurator or on demand by right-clicking a device and selecting Rediscovery.)*

Figure 12-19 shows the **Command Script Mgmt** window after devices have been selected and data collected. Table 12-5 shows the fields and buttons available.



Device	Name	Type	Release	Memory Usage
10.52.30.34	Dot34	9400	9.0.4-00	21090 / 102399 kb

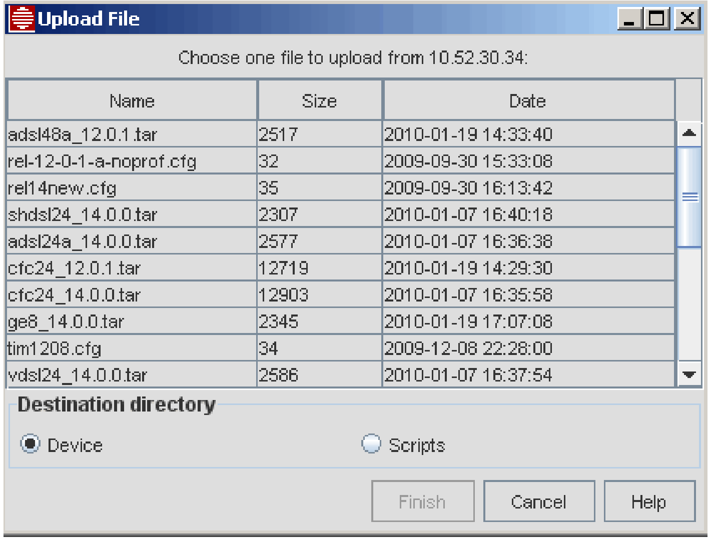
FIGURE 12-19 Command Script Mgt Window

TABLE 12-5 Command Script Mgmt Buttons/Fields

Button/Field	Description
Upload	Retrieves a file from the device. The user has to pick a file name from a list retrieved from the device. It can be stored either under the user's scripts path or under the user's device-specific in the server-side file system. Refer to "Upload File Form (Script Mgt)" on page 286.
Download	Brings up a file chooser so a file can be selected from the server file system to be downloaded all the highlighted devices. If a file already exists with the same name, it will be overwritten. This button allows files to be downloaded without being executed as a script. One use of this button is to create a login banner file, as shown in "Creating a Login Banner on a iMAP Device" on page 290.
Download/ Execute	Brings up a file chooser. A script can be selected from the server file system for execution on all the highlighted devices. After the user chooses a script, it can be downloaded on all the target devices and executed. Command feedback from the devices will be displayed in a scrolling panel. Upon completing execution, the device needs to be rediscovered in case any configuration changes were made that may affect other NMS features, like VLAN. Refer to "Download/ Execute" on page 287.
Edit Files	Brings up the unloaded multi-paged editor. The editor has open and save as buttons that work with either the local file system or the server file system, determined by a toggle on the file chooser. (Local file system is not supported in rev. 2.0) Save uses whichever file was opened, whether local or server-side. The editor also have find, find next, and cut/copy/ paste. Refer to "Edit Files" on page 289.
Delete Files	Brings up a file chooser from which the user chooses one or more files to delete. Refer to "Download Config File Window" on page 291.
Compare Files	Compares and displays two text files for comparison. Refer to "File Comparison (Text Files)" on page 342

12.2.3.1 Upload File Form (Script Mgt)

The **Upload File** form is used to retrieve a file from the device. The user has to pick a file name from a list retrieved from the device. It can be stored either under the user's scripts path or under the user's device-specific directory in the server-side file system. Refer to Figure 12-20.



Choose one file to upload from 10.52.30.34:

Name	Size	Date
adsl48a_12.0.1.tar	2517	2010-01-19 14:33:40
rel-12-0-1-a-noprof.cfg	32	2009-09-30 15:33:08
rel14new.cfg	35	2009-09-30 16:13:42
shdsl24_14.0.0.tar	2307	2010-01-07 16:40:18
adsl24a_14.0.0.tar	2577	2010-01-07 16:36:38
cfc24_12.0.1.tar	12719	2010-01-19 14:29:30
cfc24_14.0.0.tar	12903	2010-01-07 16:35:58
ge8_14.0.0.tar	2345	2010-01-19 17:07:08
tim1208.cfg	34	2009-12-08 22:28:00
vdsl24_14.0.0.tar	2586	2010-01-07 16:37:54

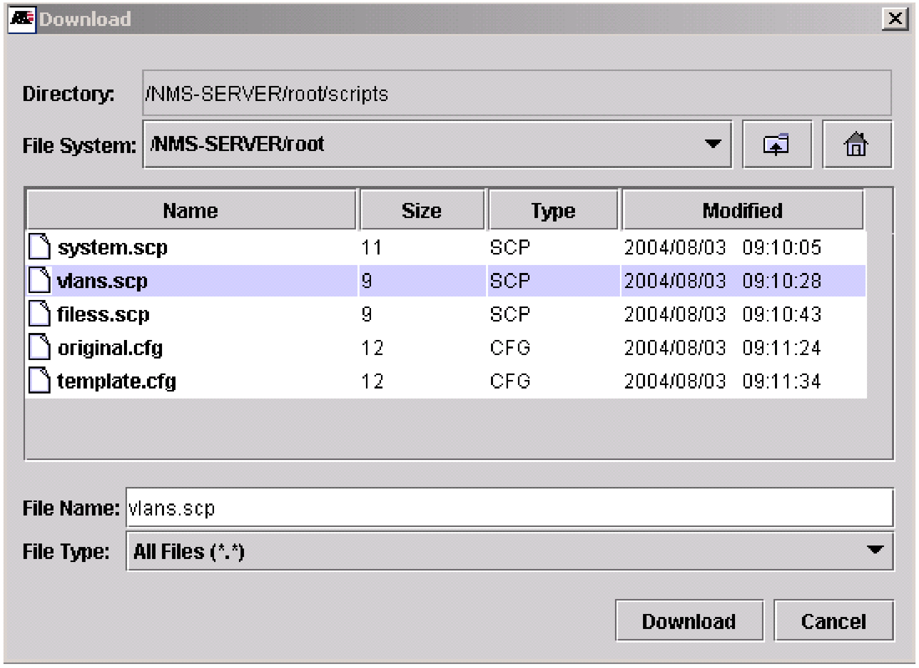
Destination directory

● Device ○ Scripts

FIGURE 12-20 Upload Window for Script Mgt Files

12.2.3.2 Download/Execute

To download and then execute script files, select one or more devices in the **Command Script Mgmt** window and click **Download/Execute**.



Directory: /NMS-SERVER/root/scripts

File System: /NMS-SERVER/root

Name	Size	Type	Modified
system.scp	11	SCP	2004/08/03 09:10:05
vlans.scp	9	SCP	2004/08/03 09:10:28
filess.scp	9	SCP	2004/08/03 09:10:43
original.cfg	12	CFG	2004/08/03 09:11:24
template.cfg	12	CFG	2004/08/03 09:11:34

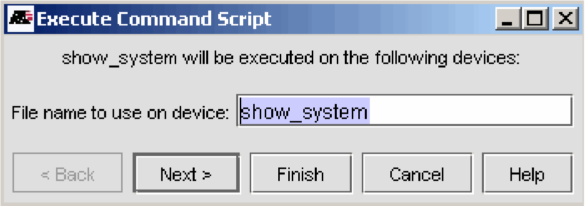
File Name: vlans.scp

File Type: All Files (*.*)

FIGURE 12-21 Download Window

After finding the appropriate file and clicking **Download**, the **Download Command Script** window appears, which lists the devices the script will be execute on, as shown in the following figure.

Note: *The blank field allows the user to specify a filename to use on device in case the server-side name is too long, missing the extension, etc. The extension must be .scp.*



show_system will be executed on the following devices:

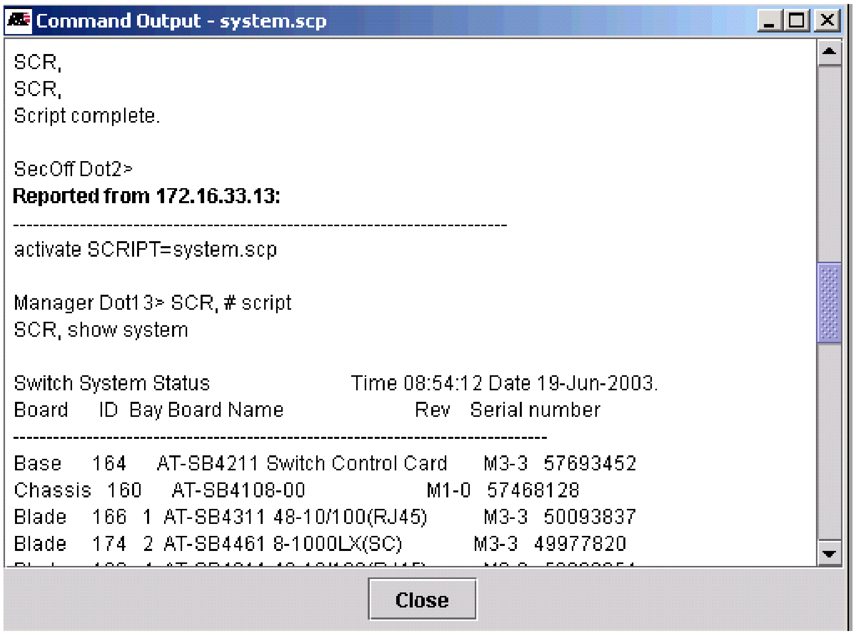
File name to use on device: show_system

FIGURE 12-22 Execute Command Script

Click **Next** to bring up the Schedule Panel, where the user can select Now (default), One Time (Schedule) or Recurring date/time.

Clicking on **Finish** begins execution immediately (Now).

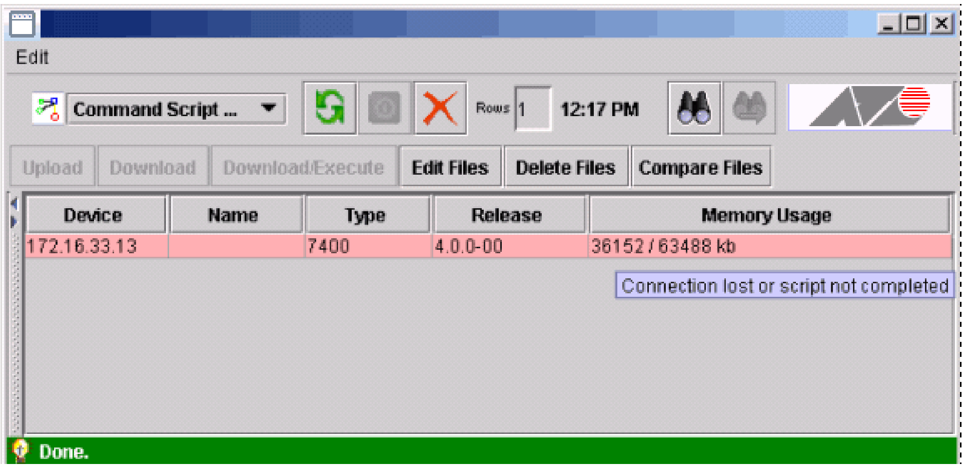
After clicking **Finish**, the script executes on the selected devices and the **Command Output** window shows the progress of the script execution. Refer to Figure 12-23.



```
SCR,
SCR,
Script complete.

SecOff Dot2>
Reported from 172.16.33.13:
--------------------------------------------------------------------------------
activate SCRIPT=system.scp

Manager Dot13> SCR, # script
SCR, show system

Switch System Status                    Time 08:54:12 Date 19-Jun-2003.
Board     ID  Bay Board Name                        Rev   Serial number
--------------------------------------------------------------------------------
Base     164    AT-SB4211 Switch Control Card      M3-3   57693452
Chassis  160    AT-SB4108-00                       M1-0   57468128
Blade    166  1 AT-SB4311 48-10/100(RJ45)          M3-3   50093837
Blade    174  2 AT-SB4461 8-1000LX(SC)             M3-3   49977820
```

FIGURE 12-23 Command Script Execution

If the network connection to the device is lost or the script fails to complete, the error **Connection Lost or script not completed** may appear in an Errors window and in the Command Script window, as shown in the following figure.



Device	Name	Type	Release	Memory Usage
172.16.33.13		7400	4.0.0-00	36152 / 63488 kb

Connection lost or script not completed

Done.

FIGURE 12-24 Failure to Run Script

Whatever script output is received up to the point of failure will be displayed in the Output Window.

Note: Since it takes several minutes before a connection times-out, there will likely be a large amount of script output (1-2 megabytes or more), which may be difficult to read. Therefore lengthy scripts should be avoided when possible.

12.2.3.3 Edit Files

The **Edit Files** button brings up the unloaded multi-paged editor, from which command scripts can be written, saved and edited. The Edit window functions are described in "Using the Edit Functions" on page 327.

For command script files, the Editor displays the contents of a Command Line Interface (CLI) script. The script file contains one or more CLI commands. Comments are identified as a hash (#) as the first character on a line. A CLI command in the script file must occupy a single line. A command cannot span more than one line. If a command requires user interaction, such as a confirmation, the user response text is included on the line after the command.

Following is a summary of the rules for creating and editing scripts:

- The commands in the script file must be syntactically correct.
- Each command must be on ONE LINE only. In other words, there is no continuation character.
- For iMAP devices, the first line of the script file must be a comment line with the word “script” in it. This is used to verify that a file is a valid script file. It is used to prevent the execution of a non-script file (i.e. load file).
- If a command returns a failure response, the script will continue to process commands following the error. It will not exit due to a parsing error OR command failure.
- If a command requires a confirmation string, the NEXT LINE must be a ‘Y’ to provide the confirmation response. If something other than a Y or N is provided, the script will quit.
- The user can provide comments (prefaced with a #) and blank lines in script files.
- The commands used must be within the realm of the user (i.e. Security Officer, Manager, User).

The contents of a script file are played back as written. Any syntax errors in the file are detected as the script is run. If an error is encountered, the device under maintenance is left in an unknown condition

12.2.3.4 Delete Command Scripts Option

The **Delete Files** button brings up the unloaded multi-paged editor, from which command scripts can be written, saved and edited. The Edit window functions are described in "Using the Delete Function" on page 332.

12.2.3.5 Compare Files

The **Compare Files** button brings up the File Comparison window, and is explained in "File Comparison (Text Files)" on page 342.

12.2.3.6 Creating a Login Banner on a iMAP Device

Command script management can be used with iMAP Devices to create a login banner. Here are the steps:

1. Use **Edit Files** to create the login banner or message-of-the-day file. This is just a text file, for example:

```
********************************************
**                            **
**        HELLO WORLD             **
**                            **
********************************************
```

2. Save the file as `motd.txt`.
3. Use **Download** to download `motd.txt` to selected iMAP devices.
4. Use **Edit Files** to create a Allied Telesis script file that assigns the login banner file, for example:

```
# script
set loginbanner file=motd.txt
```

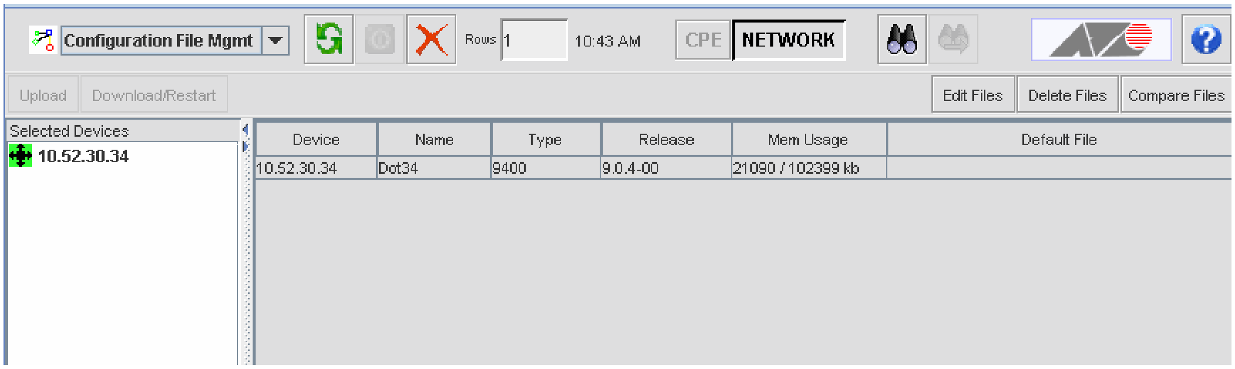
5. Use **Download/Execute** to download and execute the script on the selected iMAP devices.
6. Test by telnetting to one of the selected iMAP devices and observe the login banner.

12.2.4 Configuration File Management

For Rapier and iMAP devices, the configuration file is an ASCII-formatted file that contains the complete configuration of the device. When the device is rebooted, the configuration file can replace the currently active (running) configuration.

Note: *Significant configuration changes made using configuration files will not be reflected in the NMS until the devices are rediscovered. (Rediscovery can occur automatically as configured in Discovery Configurator or on demand by right-clicking a device and selecting Rediscovery.)*

After selecting the application **Configuration File Mgmt** and collecting data for the selected devices, the user will see the panel shown in Figure 12-25. Table 12-6. shows the fields/buttons available.



Device	Name	Type	Release	Mem Usage	Default File
10.52.30.34	Dot34	9400	9.0.4-00	21090 / 102399 kb	

FIGURE 12-25 Configuration File Mgt Panel

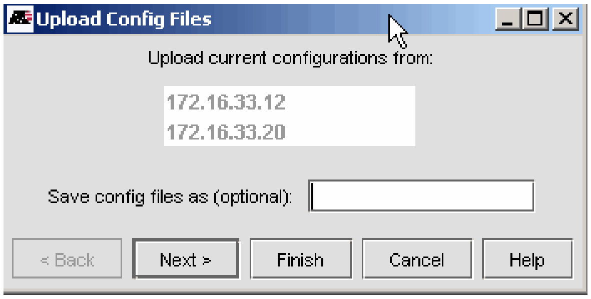
TABLE 12-6 Configuration Mgt Buttons/Fields

Option	Description
Upload	This brings up the Upload Config Files Form, which allows the user to back up the file to a directory on the AlliedView NMS server. Refer to "Upload Config Files Window" on page 291.
Download/Restart	This brings up the Download Config File form, which allows the user to restore a configuration file. Refer to "Download Config File Window" on page 291.
Edit Files	This brings up the multi-paged text editor Refer to "Edit Window" on page 292.
Delete Files	This brings up a directory window, which allows the user to delete a file. Refer to "Delete Window" on page 292.
Compare Files	This brings up the File Comparison tool. Refer to "File Comparison (Text Files)" on page 342

12.2.4.1 Upload Config Files Window

The **Upload Config Files** window provides a backup function. The filename is optional. If left blank, a name will be generated based on the date and time. If a filename is entered by the user, any name is allowed since it will be saved on the server file system.

If multiple devices are selected, their configuration files will all be stored using the same filename, with each file under its device name. Refer to Figure 12-26.



Upload current configurations from:

172.16.33.12
172.16.33.20

Save config files as (optional):

FIGURE 12-26 Upload Window for Configuration Mgt Files

Click **Next** to bring up the Schedule Panel, where the user can select Now (default), One Time (Schedule) or Recurring date/time.

Clicking on **Finish** begins execution immediately (Now).

Note: *Blank names are suitable for recurrent uploads since new names will be chosen by the system as uploads are performed. If you enter a name and specify recurrent uploads, the same name will be used and the files will be overwritten.*

12.2.4.2 Download Config File Window

The **Download Config File** window provides a restore function.The user is prompted to select a file name from a list of files for the highlighted devices. This window works as follows:

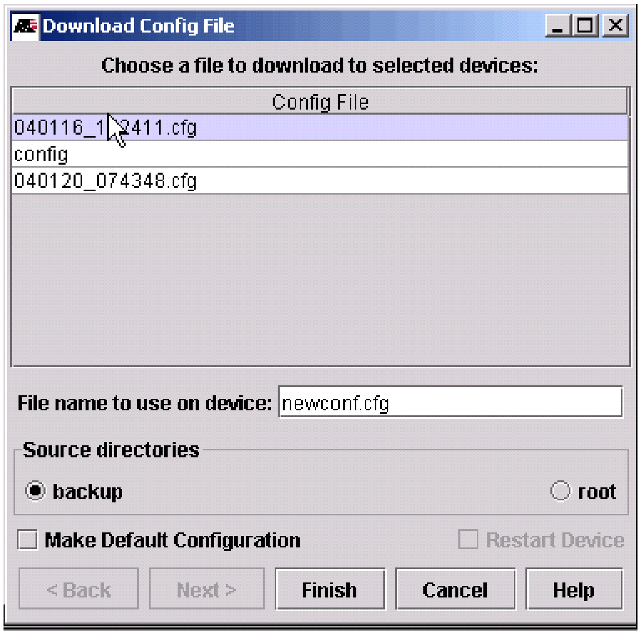
- All files with the same names for the selected devices are displayed.
- One commonly-named set of files can be selected for download to selected devices. If any device doesn't have a file name shared by all the others, then none will be available for selection. When this happens, the list will be initially empty.
- When downloaded, separate files are downloaded from respective device-specific directories to each device. The files may be renamed during download by entering a new name in the text field below the table. If the name is incorrectly formatted, download attempts will be cancelled and an error message will popup.

- The Source directories option determines whether they are downloaded form the **backup** subtree or from the user's (root) device subtree. When the source directory is changed, the list of files will change accordingly. Whenever such a change results in an empty list, a warning message will appear.

Note: *If one or more iMAPs are included in the device selection, the* **backup** *option is unavailable, since Configuration File Management is for text-based files, and iMAP backup files are database files in binary format. The user's subtree will contain the text config files that were uploaded using this application.*

- If **Make default configuration** is selected, the downloaded files will become the default configurations on the devices (applied the next time the devices are rebooted).
- If **Restart** is selected, the device will be rebooted upon completion of the download

Note: *Once the download is complete, rediscover the device to ensure the data in the configuration file is communicated to the AlliedView NMS.*


Download Config File

Choose a file to download to selected devices:

Config File
040116_1_2411.cfg
config
040120_074348.cfg

File name to use on device: newconf.cfg

Source directories

● backup ○ root

□ Make Default Configuration □ Restart Device

FIGURE 12-27 Download Config File Form - From Backup Directory

12.2.4.3 Edit Window

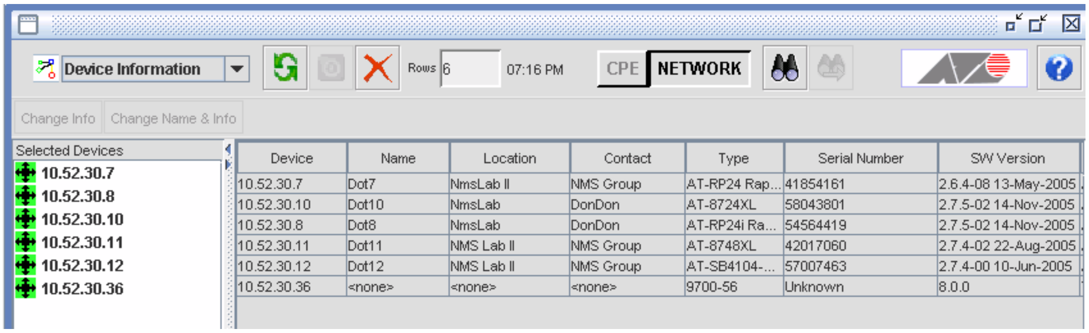
This **Edit** window has the same functions for Configuration and Script files, and is described in "Using the Edit Functions" on page 327.

12.2.4.4 Delete Window

The **Delete** window brings up a list of configuration files for the selected device(s), from which the user may delete, and is described in "Using the Delete Function" on page 332.

12.2.5 Device Information

This application allows identification information (name, location, and contact information) to be changed. After selecting the application and collecting data for the selected devices, the user will see the following figure.

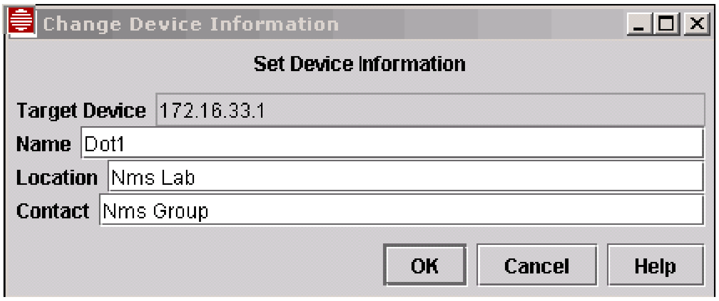


Selected Devices
10.52.30.7
10.52.30.8
10.52.30.10
10.52.30.11
10.52.30.12
10.52.30.36

Device	Name	Location	Contact	Type	Serial Number	SW Version
10.52.30.7	Dot7	NmsLab II	NMS Group	AT-RP24 Rap...	41854161	2.6.4-08 13-May-2005
10.52.30.10	Dot10	NmsLab	DonDon	AT-8724XL	58043801	2.7.5-02 14-Nov-2005
10.52.30.8	Dot8	NmsLab	DonDon	AT-RP24i Ra...	54564419	2.7.5-02 14-Nov-2005
10.52.30.11	Dot11	NMS Lab II	NMS Group	AT-8748XL	42017060	2.7.4-02 22-Aug-2005
10.52.30.12	Dot12	NMS Lab II	NMS Group	AT-SB4104-...	57007463	2.7.4-00 10-Jun-2005
10.52.30.36	<none>	<none>	<none>	9700-56	Unknown	8.0.0

FIGURE 12-28 Device Information Application

When one device is chosen the **Change Name & Info** button is activated, and clicking it brings up the **Change Device Information** window, as shown in Figure 12-29. (Double-clicking the device row will also bring up this form.)



Target Device 172.16.33.1
Name Dot1
Location Nms Lab
Contact Nms Group

FIGURE 12-29 Change Device Information Window

In this window the **Name**, **Location** and **Contact** can be changed.

When more than one device is chosen, the **Change Info** button is activated; clicking it also brings up the **Change Device Information** window, but only the Location and Contact information can be changed.

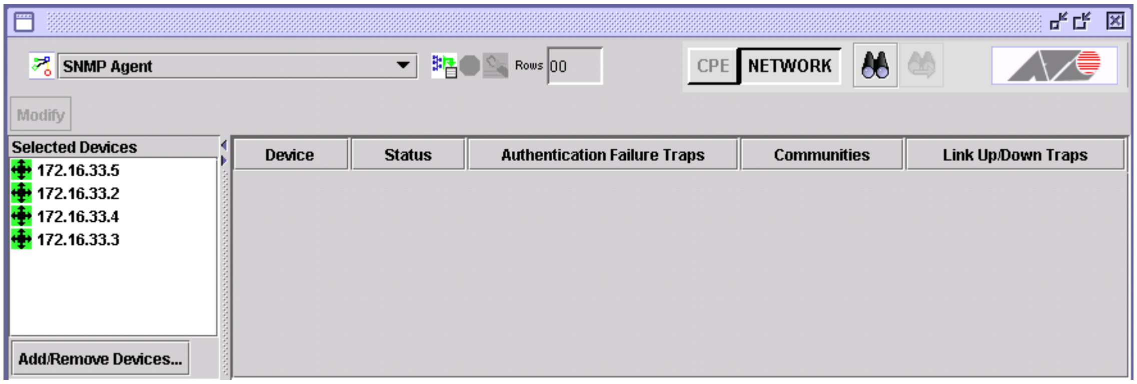
12.2.6 SNMP Agent

The Simple Network Management Protocol (SNMP) involves the device agent, which controls the managed objects in the device.

This application is used to configure the SNMP agent that sends SNMP traps to the AlliedView NMS or other hosts, as well as configure SNMP communities.

When the SNMP Agent application is chosen the following figure appears.

Note: *When going from one application to another, and the next application has not yet been used, the devices that were in the first application are carried over to the second, which is why the three devices from backup/restore are now selected in the SNMP Agent Panel.*

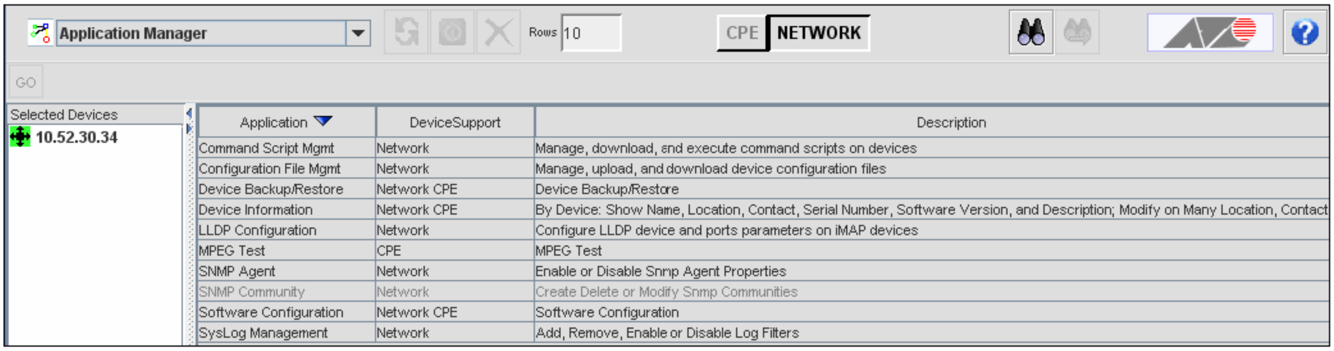


Selected Devices
- 172.16.33.5
- 172.16.33.2
- 172.16.33.4
- 172.16.33.3

Device	Status	Authentication Failure Traps	Communities	Link Up/Down Traps

FIGURE 12-30 SNMP Agent Panel - Initial View

After clicking **Add/Remove Devices**, (if necessary) and clicking the **Collect Data** icon, data is gathered for the devices and the following figure appears.

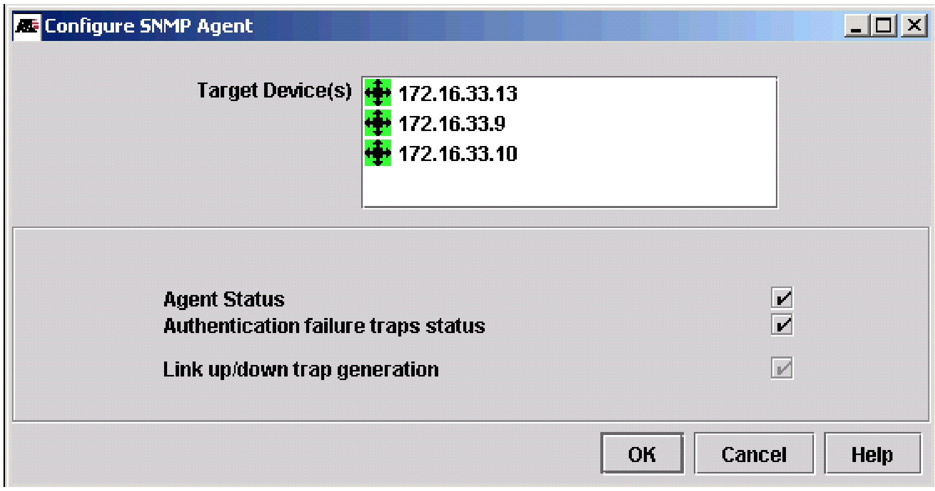


Selected Devices
- 10.52.30.34

Application	DeviceSupport	Description
Command Script Mgmt	Network	Manage, download, and execute command scripts on devices
Configuration File Mgmt	Network	Manage, upload, and download device configuration files
Device Backup/Restore	Network CPE	Device Backup/Restore
Device Information	Network CPE	By Device: Show Name, Location, Contact, Serial Number, Software Version, and Description; Modify on Many Location, Contact
LLDP Configuration	Network	Configure LLDP device and ports parameters on iMAP devices
MPEG Test	CPE	MPEG Test
SNMP Agent	Network	Enable or Disable Snmp Agent Properties
SNMP Community	Network	Create Delete or Modify Snmp Communities
Software Configuration	Network CPE	Software Configuration
SysLog Management	Network	Add, Remove, Enable or Disable Log Filters

FIGURE 12-31 SNMP Agent Panel

To modify the agent for one or more devices, select the rows, and then click **Modify** (now active). The following figure appears.



Target Device(s)
- 172.16.33.13
- 172.16.33.9
- 172.16.33.10

Agent Status ☑
Authentication failure traps status ☑
Link up/down trap generation ☑

FIGURE 12-32 Configure SNMP Agent Panel

The following table lists the options available.

TABLE 12-7 SNMP Agent Fields

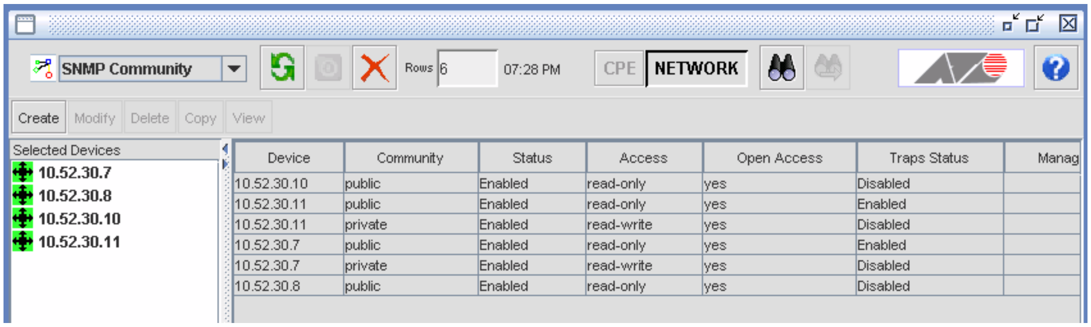
Option	Description
Agent status	A checkbox to enable or disable the device(s). A dark check means all selected devices have this feature enabled, an unchecked box means no devices have this feature enabled, and a gray checkbox means some devices have this feature enabled and some devices do not.
Authentication failure traps status	A checkbox to enable or disable the create traps when an unauthorized attempt has been made.
Link up/down trap generation (all interfaces)	A checkbox to set each interface to send (checked) or not send (not checked) a trap when its up/down state changes. A gray box means no changes are made.
OK	Applies the changes.
Cancel	Cancels the changes made in this window.
Help	Invokes online help.

12.2.7 SNMP Community

An SNMP community helps to define the relationship between the AlliedView NMS and the Management Information Base (MIB) of the device, in essence defining the operations that can be performed on various objects in the device. For each device there may be multiple communities, with each community providing a set of operations.

Caution: In SNMP, a community name acts as a password; if the community includes write operations, it is possible for other applications to use the community name and change the values for a switch configuration.

When the SNMP Agent application is chosen and the Collect Data icon is clicked, the following figure appears.

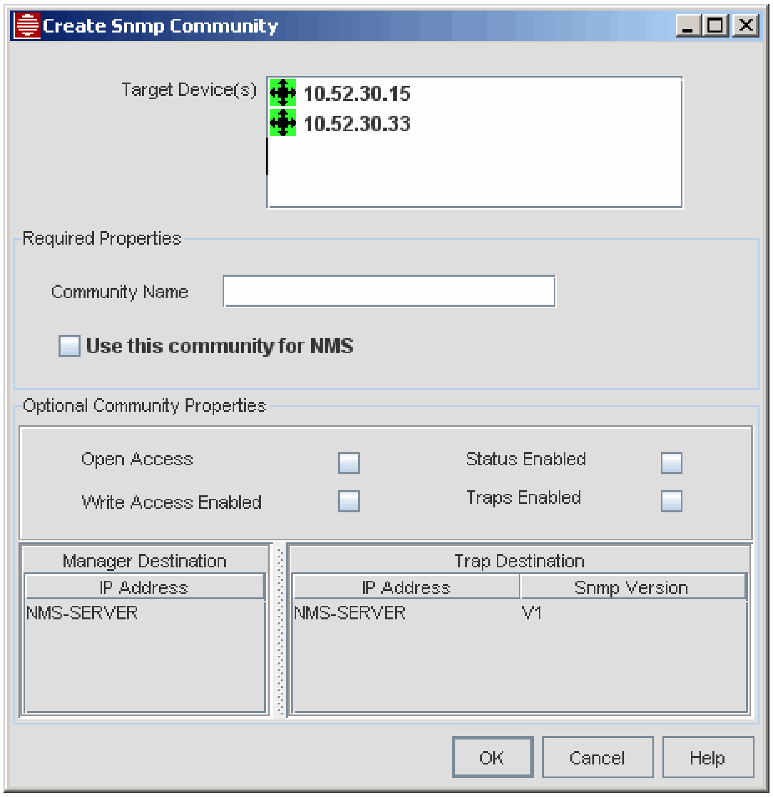


Device	Community	Status	Access	Open Access	Traps Status	Manag
10.52.30.10	public	Enabled	read-only	yes	Disabled	
10.52.30.11	public	Enabled	read-only	yes	Enabled	
10.52.30.11	private	Enabled	read-write	yes	Disabled	
10.52.30.7	public	Enabled	read-only	yes	Enabled	
10.52.30.7	private	Enabled	read-write	yes	Disabled	
10.52.30.8	public	Enabled	read-only	yes	Disabled	

FIGURE 12-33 SNMP Community Panel

At this point a new community can be created, or the devices can be selected and the community settings can be modified, removed, or copied. The **Create**, **Modify**, and **Copy** buttons perform these functions. The following figures shows the **Create**, **Modify**, and **Copy** SNMP Community forms, which are displayed when these buttons are clicked.

Caution: Creating, modifying, and deleting SNMP Communities for devices managed by the NMS must be done via the NMS and not the device CLI. Making changes using the device CLI will cause a data mismatch between the device and the NMS database. If you must make changes using the device CLI, you must also make the changes in the NMS.



Create Snmp Community

Target Device(s)
10.52.30.15
10.52.30.33

Required Properties

Community Name

☐ Use this community for NMS

Optional Community Properties

Open Access	☐	Status Enabled	☐
Write Access Enabled	☐	Traps Enabled	☐

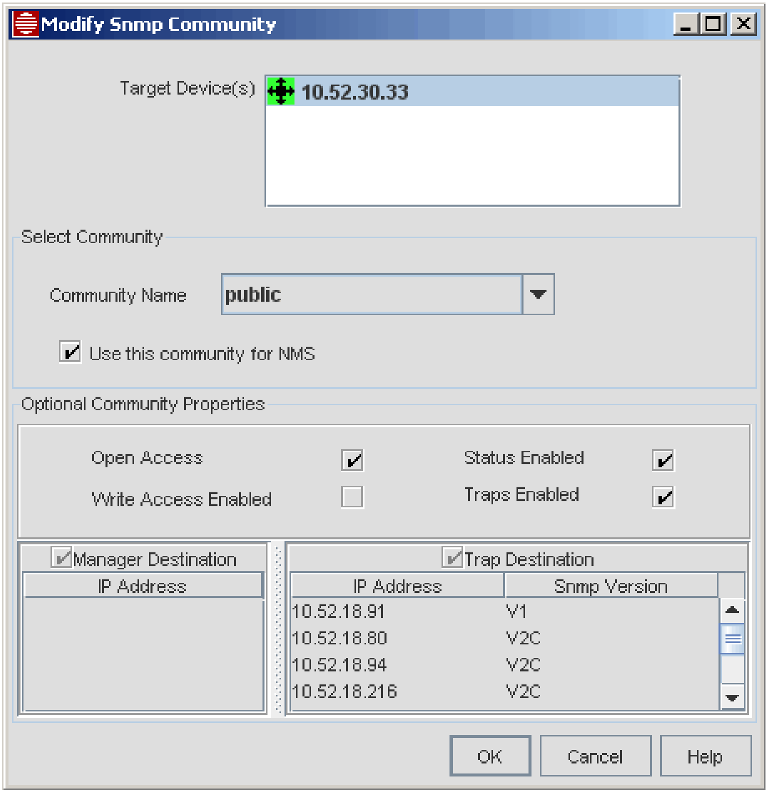
Manager Destination

IP Address
NMS-SERVER

Trap Destination

IP Address	Snmp Version
NMS-SERVER	V1

FIGURE 12-34 Create SNMP Community Form



Modify Snmp Community

Target Device(s)
10.52.30.33

Select Community

Community Name: public

☑ Use this community for NMS

Optional Community Properties

Open Access	☑	Status Enabled	☑
Write Access Enabled	☐	Traps Enabled	☑

☑ Manager Destination

IP Address

☑ Trap Destination

IP Address	Snmp Version
10.52.18.91	V1
10.52.18.80	V2C
10.52.18.94	V2C
10.52.18.216	V2C

FIGURE 12-35 Modify SNMP Community Form

When the **Copy** button is clicked, a two-page form appears. Both pages are shown in the following figures.

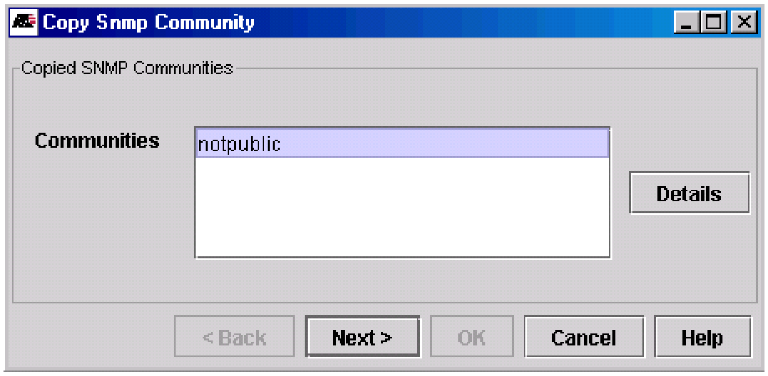


FIGURE 12-36 Copy SNMP Community Form (First Page) - File

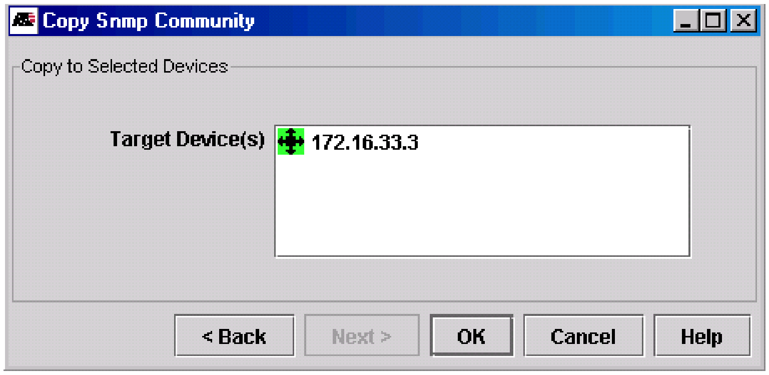


FIGURE 12-37 Copy SNMP Community Form (Second Page) - File

The following table lists the options available.

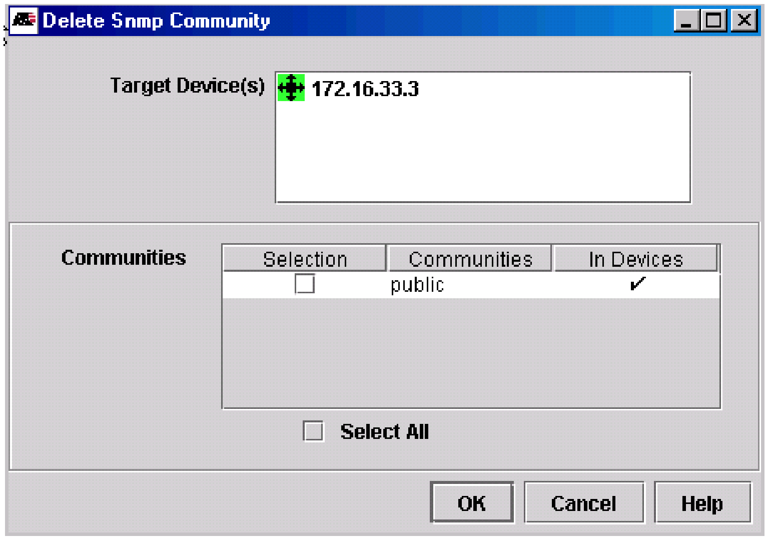
TABLE 12-8 Community Configuration Fields

Option	Description
Community Name	A text box when adding (creating) a community name, a drop-down of community names when modifying a community name. When adding a community, clicking on the Add/Remove button adds the community. If a community is already highlighted, clicking on the Add/Remove button will remove the community for the device.
Use this community for NMS	Make this community be used for SNMP communication.
Open Access	Checkbox to allow Open Access or not for this community.
Status Enabled	Checkbox to enable or disable status messaging for this community.
Traps Enabled	Checkbox to enable or disable the ability for this community to produce traps.
Write Access Enabled	Checkbox to enable Read-Only or Read-Write Access for this community.
Manager Destination	The IP address of the snmp Manager. If Open Access is not enabled (not checked), then GETs are only accepted from this IP address. If Open Access is checked, this field is not used. When the check mark is black, all Managers in the list are added to the devices. When the check mark is gray, only the new Managers in the list are added to the devices. If unchecked, no changes are made.

TABLE 12-8 Community Configuration Fields

Option	Description
Trap Destination	The available trap host. This is the IP address where traps are to be sent, and the SNMP version (pull down) of which version. When the check mark is black, all trap hosts in the list are added to the devices. When the check mark is gray, only the new trap hosts in the list are added to the devices. If unchecked, no changes are made.
Help	Invokes context-sensitive online help.
OK	Activates changes.
Cancel	Cancels changes.

To delete a community, select one or more devices and click on **Delete**.



Selection	Communities	In Devices
□	public	✓

FIGURE 12-38 Delete Snmp Community Window

The user can then select the communities for the **Target Device** (or **Select All**) and by clicking **OK**, delete those communities.

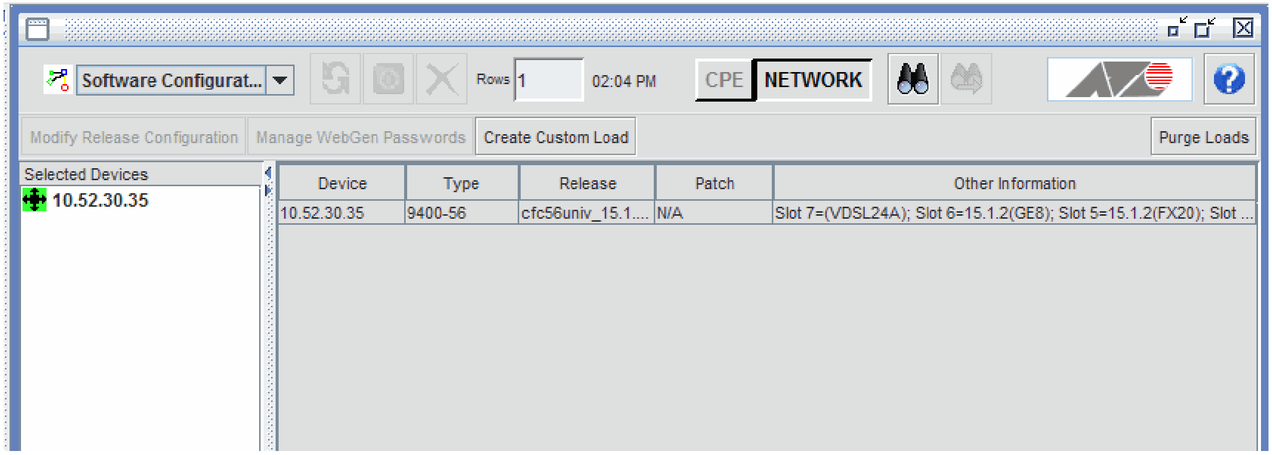
12.2.8 Obtaining Software Loads

The NMS manages software updates to devices. When you have a new software load, place it in the `<NMS_Home>/swdownload` directory. If the software requires a license, place the license certificate file in the directory with the software load.

Note: For information on obtaining software licenses and certificate files, contact Allied Telesis customer support.

12.2.9 Standard Load Software Configuration

When the *Software Configuration* application is chosen and the **Collect Data** icon is clicked, the following figure appears.



Device	Type	Release	Patch	Other Information
10.52.30.35	9400-56	cfc56univ_15.1....	N/A	Slot 7=(VDSL24A); Slot 6=15.1.2(GE8); Slot 5=15.1.2(FX20); Slot ...

FIGURE 12-39 Software Configuration Panel

12.2.9.1 Firmware Decoupling Feature as part of Software Configuration

To reduce the install size for the NMS installation load, firmware loads for devices are separate from the installation load. The user instead adds device firmware loads to the NMS server.

Release files for closely related device types and releases are placed together as a bundle, so a file is a bundle that can consist of multiple groups placed together in one zip file. Within this zip file is an xml file that:

- Allows the NMS to determine compatibility for the file with the release installed on the NMS.
- Allows the user to identify the family, device types, versions, descriptions, and release date.

Moreover, when a point release is added, the NMS determines which versions are obsolete, so that only those current firmware loads are available and obsolete firmware loads can be purged.

The firmware is ready to load and use as soon as it is uploaded, without the need to restart the server.

To add a firmware file to the NMS:

1. Learn about the latest firmware releases from Allied Telesis.
2. Obtain the file(s) using an ftp/web site.
3. Transfer the file(s) to the NMS server.
4. Use the Software Configuration feature to add and delete files. The NMS looks at the downloaded files and determines which files are compatible, then determines which files can be downloaded onto the devices and which ones can be purged as obsolete.
5. Choose the Modify Release Configuration, and the files, if compatible, are included in the download.
6. Alternatively, choose Purge Files. The NMS highlights which files are obsolete and gives you the ability to highlight all obsolete files which can then be deleted. (You can still delete current files if desired.)

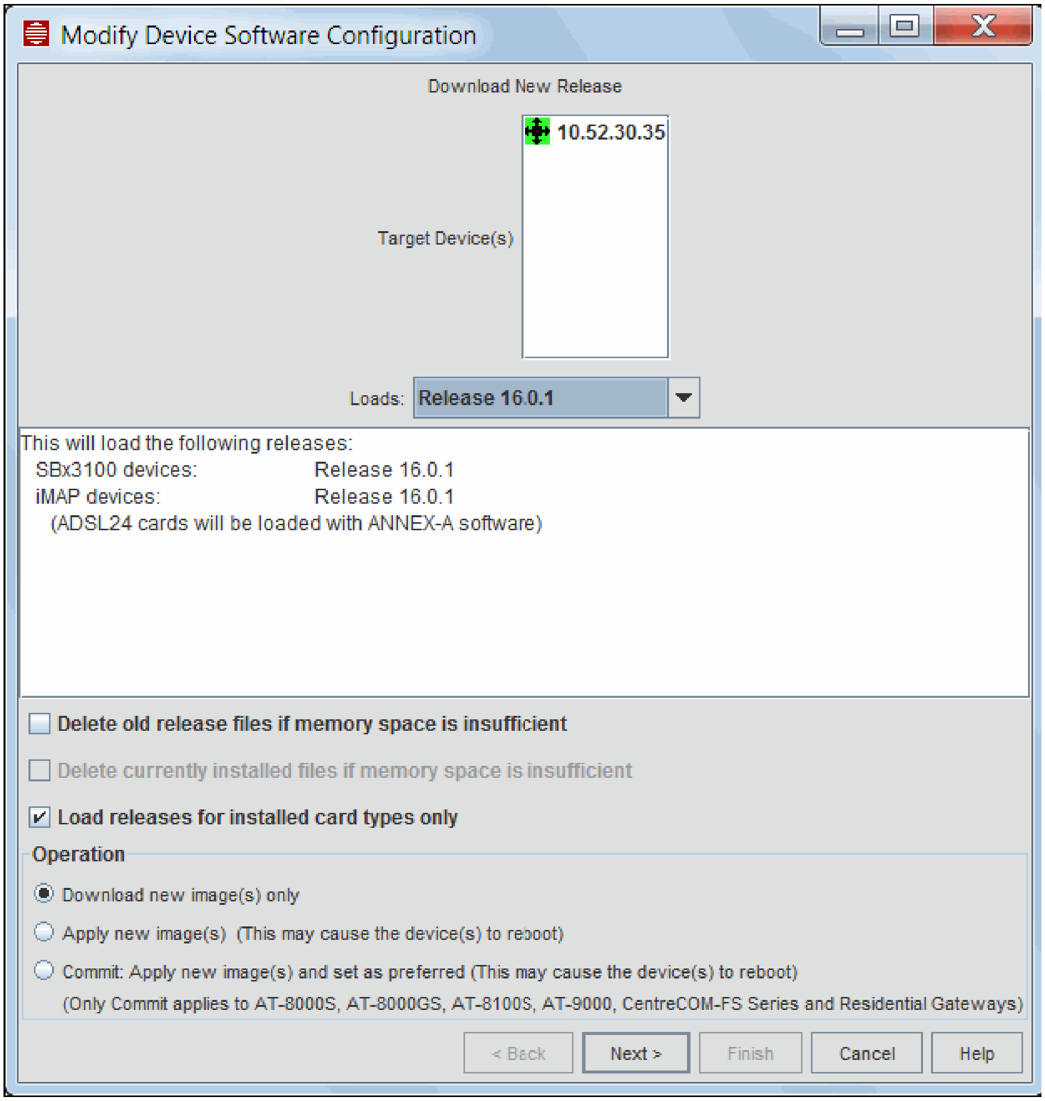
The rest of this subsection goes through the Software Configuration and highlights where the Firmware Decoupling feature is used.

12.2.9.2 Modifying Software Configuration

The table shows for the selected devices all of the filetypes for the devices. When the user selects the devices and clicks **Modify Release Configuration**, the **Modify Release Configuration** form appears, as shown in the following figure.

Caution: *For the devices that will receive downloads, do not set their telnet idle session time-out to any value less than 6 minutes. This minimum is needed to ensure the NMS is aware the download is complete and can proceed with any further steps.*

Note: If a custom load has been built (refer to "Custom Load Software Configuration" on page 303), it will be added to Loads pull-down.



Modify Device Software Configuration

Download New Release

Target Device(s) 10.52.30.35

Loads: Release 16.0.1

This will load the following releases:

SBx3100 devices:	Release 16.0.1
iMAP devices:	Release 16.0.1

(ADSL24 cards will be loaded with ANNEX-A software)

□ Delete old release files if memory space is insufficient

□ Delete currently installed files if memory space is insufficient

☑ Load releases for installed card types only

Operation

● Download new image(s) only

○ Apply new image(s) (This may cause the device(s) to reboot)

○ Commit: Apply new image(s) and set as preferred (This may cause the device(s) to reboot)
(Only Commit applies to AT-8000S, AT-8000GS, AT-8100S, AT-9000, CentreCOM-FS Series and Residential Gateways)

FIGURE 12-40 Modify Software Device Configuration Panel

Table 12-9 lists the options available.

TABLE 12-9 Software Download Buttons/Fields

Option	Description
Loads	A pull-down menu for choosing the software release for the device. For iMAP devices, the user can select loads that assume Annex A or Annex B cards are being loaded.
Delete old release files if space needed	A checkbox that tells the device to delete old release files before loading the chosen release file. (Note that you may need to check this box if a previous download of a release file to the device has failed.)

TABLE 12-9 Software Download Buttons/Fields (Continued)

Option	Description
Delete current release files if space needed	A checkbox that is active only after choosing the checkbox to delete old release files, it tells the device to delete the current release file as well as old release files. (Note that you may need to check this box if a download of the release file using the first checkbox has failed.)
Load releases for installed card types only	This option appears whenever any of the target devices is an iMAP. iMAP devices may support numerous card types, and checking this option will only load the release files for currently installed card types, saving memory. If a new card type is installed afterwards, the downloads will have to be re-executed to update the release for the new card.
Operation	A set of radio buttons for choosing which download method to use. **Download new image(s) only** places the selected image(s) on the device. **Apply new image(s)** places the selected image(s) on the device and restarts the device with the downloaded image(s) only if necessary. When the device restarts again, it will revert to the previous image(s). **Apply new image(s) and set as preferred** places the selected image(s) on the device and restarts the device with the downloaded image(s) only if necessary. When the device restarts again, it will keep the downloaded images as the active ones and not revert to the previous image(s).
Next	Brings up the schedule panel for recurring backups.
Finish	Submits the Task name and all options for processing immediately.
Cancel	Closes the window. If the Submit button has not been pressed, any changes to the form are lost.
Help	Invokes online help.

Note: When a device cold starts and sends a cold trap, the device will be automatically rediscovered within two minutes, so after a software download the information for a device will be automatically updated (although it may be out of synch for a short time).

Note: In the unlikely event of getting an "NMS File System Error", see the trace log for more detailed and more specific error message. This error only occurs when NMS was not installed properly, the FTP service is not configured properly, the NMS file system is full or corrupt, or the NMS server account has been changed to revoke required read/write/delete file access privileges.

12.2.9.3 Purge Load Files

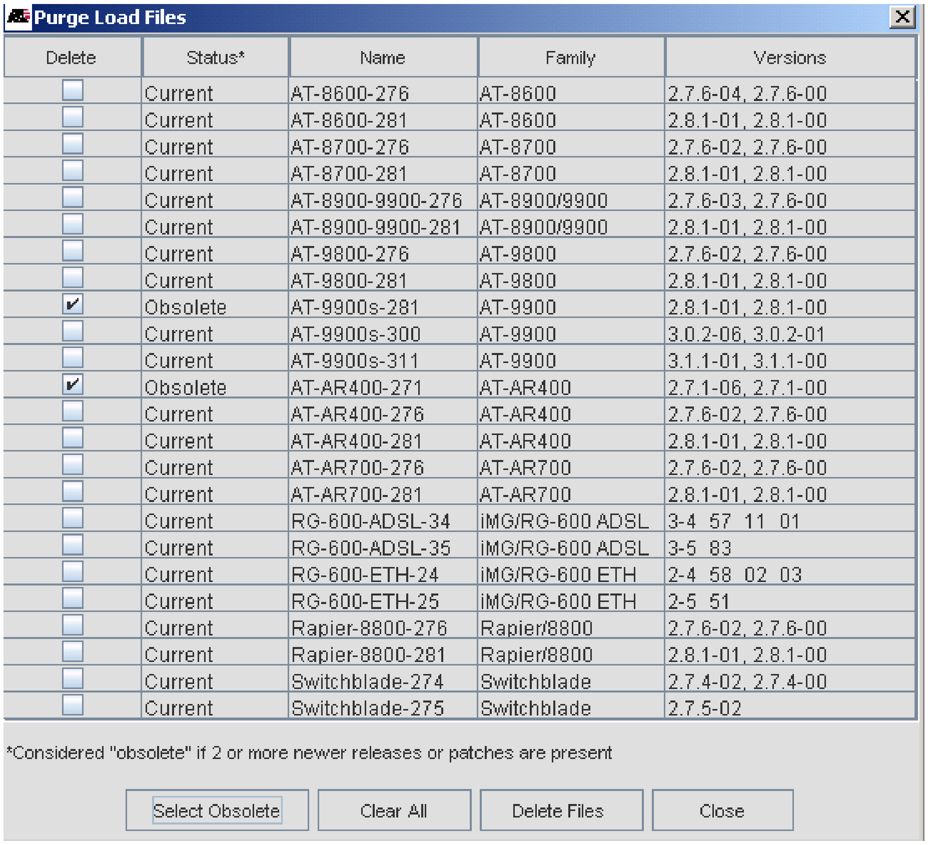
The Purge Load Panel lists all the load bundles and gives a summary of their contents. Older load bundles can be selected for deletion. **When deleted, all files making up the load bundle will be deleted**.

"Obsolete" bundles are bundles in which all files are superseded by 2 or more versions from other bundles. Any bundle can be deleted any time, but "obsolete" bundles are pre-selected for convenience.

The **Select Obsolete** button selects (checks) all rows containing obsolete bundles.

The **Clear All** button, un-selects (unchecks) all rows.

The **Delete Files** button deletes all files from all selected (checked) bundles. If any errors occur during the deletion, an error dialog will pop up with an error message.



Delete	Status*	Name	Family	Versions
☐	Current	AT-8600-276	AT-8600	2.7.6-04, 2.7.6-00
☐	Current	AT-8600-281	AT-8600	2.8.1-01, 2.8.1-00
☐	Current	AT-8700-276	AT-8700	2.7.6-02, 2.7.6-00
☐	Current	AT-8700-281	AT-8700	2.8.1-01, 2.8.1-00
☐	Current	AT-8900-9900-276	AT-8900/9900	2.7.6-03, 2.7.6-00
☐	Current	AT-8900-9900-281	AT-8900/9900	2.8.1-01, 2.8.1-00
☐	Current	AT-9800-276	AT-9800	2.7.6-02, 2.7.6-00
☐	Current	AT-9800-281	AT-9800	2.8.1-01, 2.8.1-00
☑	Obsolete	AT-9900s-281	AT-9900	2.8.1-01, 2.8.1-00
☐	Current	AT-9900s-300	AT-9900	3.0.2-06, 3.0.2-01
☐	Current	AT-9900s-311	AT-9900	3.1.1-01, 3.1.1-00
☑	Obsolete	AT-AR400-271	AT-AR400	2.7.1-06, 2.7.1-00
☐	Current	AT-AR400-276	AT-AR400	2.7.6-02, 2.7.6-00
☐	Current	AT-AR400-281	AT-AR400	2.8.1-01, 2.8.1-00
☐	Current	AT-AR700-276	AT-AR700	2.7.6-02, 2.7.6-00
☐	Current	AT-AR700-281	AT-AR700	2.8.1-01, 2.8.1-00
☐	Current	RG-600-ADSL-34	iMG/RG-600 ADSL	3-4 57 11 01
☐	Current	RG-600-ADSL-35	iMG/RG-600 ADSL	3-5 83
☐	Current	RG-600-ETH-24	iMG/RG-600 ETH	2-4 58 02 03
☐	Current	RG-600-ETH-25	iMG/RG-600 ETH	2-5 51
☐	Current	Rapier-8800-276	Rapier/8800	2.7.6-02, 2.7.6-00
☐	Current	Rapier-8800-281	Rapier/8800	2.8.1-01, 2.8.1-00
☐	Current	Switchblade-274	Switchblade	2.7.4-02, 2.7.4-00
☐	Current	Switchblade-275	Switchblade	2.7.5-02

*Considered "obsolete" if 2 or more newer releases or patches are present

FIGURE 12-41 Purge Load Files

12.2.9.4 Using a MTAC Account and WebGen (Manual) to Enable Software Upgrades

To enable software upgrades for Rapier devices, a two-step process is used that involves tasks at an Allied Telesis website as well as a AlliedView NMS feature:

1. The Multi-Time-Access-Code (MTAC) is a website where customers can register themselves and then set up for their devices (based on the serial numbers) the OSs that will be loaded.
2. The **WebGen Import** Form tool (on the AlliedView NMS) is then brought up, and the results from the MTAC account are copied either directly into the form or are copied into a file so that it can be copied into the form later.

To access your MTAC account, go to https://licence.alliedtelesis.co.nz/mtac/fusebox.cfm.

Note: Before accessing this site, you will need to obtain a valid user ID and password from your authorized Allied Telesis representative or reseller.

Once you have accessed the site, you will go through a series of forms where you enter your id, password, give general customer details, and correlate an OS with the serial numbers of your devices. You must also fill in details on the device for each serial number. (Note that you do not have to enter information for all your devices and can revisit your account later.) After clicking **Generate**, a list of ENABLE commands is produced that selects the OS for the devices and include the passwords.

Note: For detailed instructions on using your MTAC account to generate licences, see www.alliedtelesis.co.nz/webgen/pdf/webgen-customer-guide.pdf.

Once you have this list of commands generated with the account, you can use the results in one of two ways:

- Save the html form as a filename. This file can then be transferred to the NMS if there is no internet access from the NMS server. The WebGen Import form is then used to access this file so it can be imported.
- The WebGen Import form is brought up and the results are pasted directly into the form and imported.

To access the WebGen Import Form, use the Start Menu and Select *Programs -> <NMS Load> -> Tools*. This will bring up the WebGen Import form shown in the following figure.

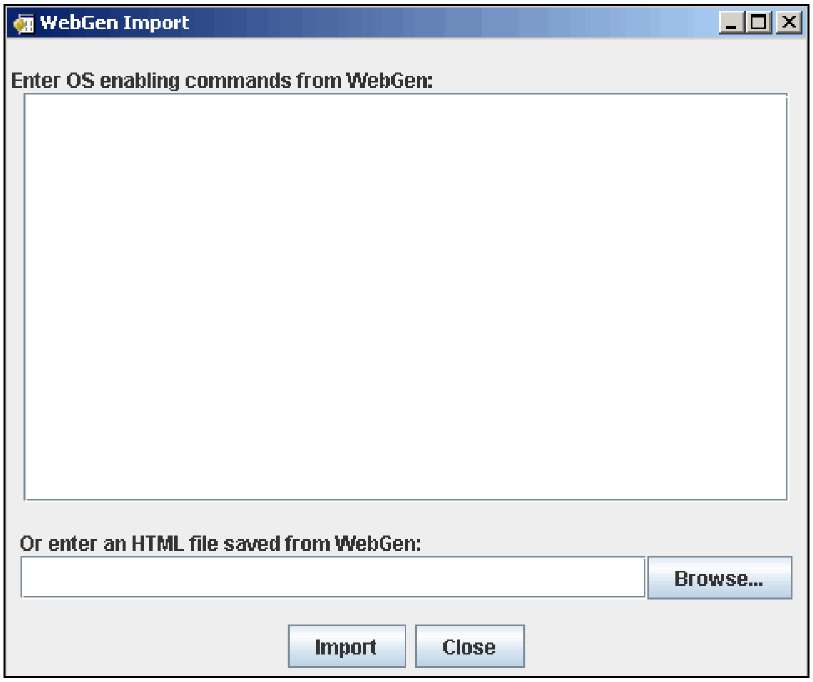

WebGen Import
Enter OS enabling commands from WebGen:
Or enter an HTML file saved from WebGen:
Browse...
Import
Close

FIGURE 12-42 WebGen Import Form

To use the WebGen form directly, paste the results of the Generate command directly into the form and then Select **Import**. A pop-up window will appear indicating that the passwords were successfully imported, so that during software downloads performed at the NMS, the ENABLE commands with the passwords are already included.

To use a saved file, type in the name of the file or (more likely) use the **Browse** button and locate the file. Select Import, and the same message and action occurs as when using the form directly.

If any errors occur during parsing, a dialog box will appear indicating the error condition.

Note: To easily gather device attributes so they may be copied and pasted in WebGen, the user can create a Custom View of the Network Inventory/Nodes component and have only the selected devices with the selected attributes appear. This would mean changing either the Select Props to View or Additional Props to match what you wish to capture. You can then select the row with the mouse, use Control-C to copy, then go to the appropriate window and Control-V to paste.

12.2.10 Custom Load Software Configuration

The Custom load configuration is entered from the Software Configuration application using the **Create Custom Load** button, as shown in Figure 12-39, at the beginning of this subsection on Software Configuration. This button is device independent and therefore enabled with or without any devices selected.

Selecting the **Create Custom Loads** button brings up the The **Custom Device Loads** Form, as shown in Figure 12-43. This shows all the device loads. Load names and types are listed in a table, which can be sorted by clicking on a column heading. Double clicking a column heading puts the table back in its unsorted order, which is usually with the newest loads at the bottom.

Loads are groups of device configurations that can be selected when downloading software releases to devices. Loads types are:

- Standard - The standard loads are pre configured in the NMS release and can be viewed in detail but neither modified nor deleted.
- Custom - Custom loads are created by users and can be added, modified, viewed, and deleted, which are the tasks that make up this feature.

The **Modify** button allows modifying a description. Select a custom load from the table, modify the description, and then press the Modify button. (Names cannot be modified after creation)

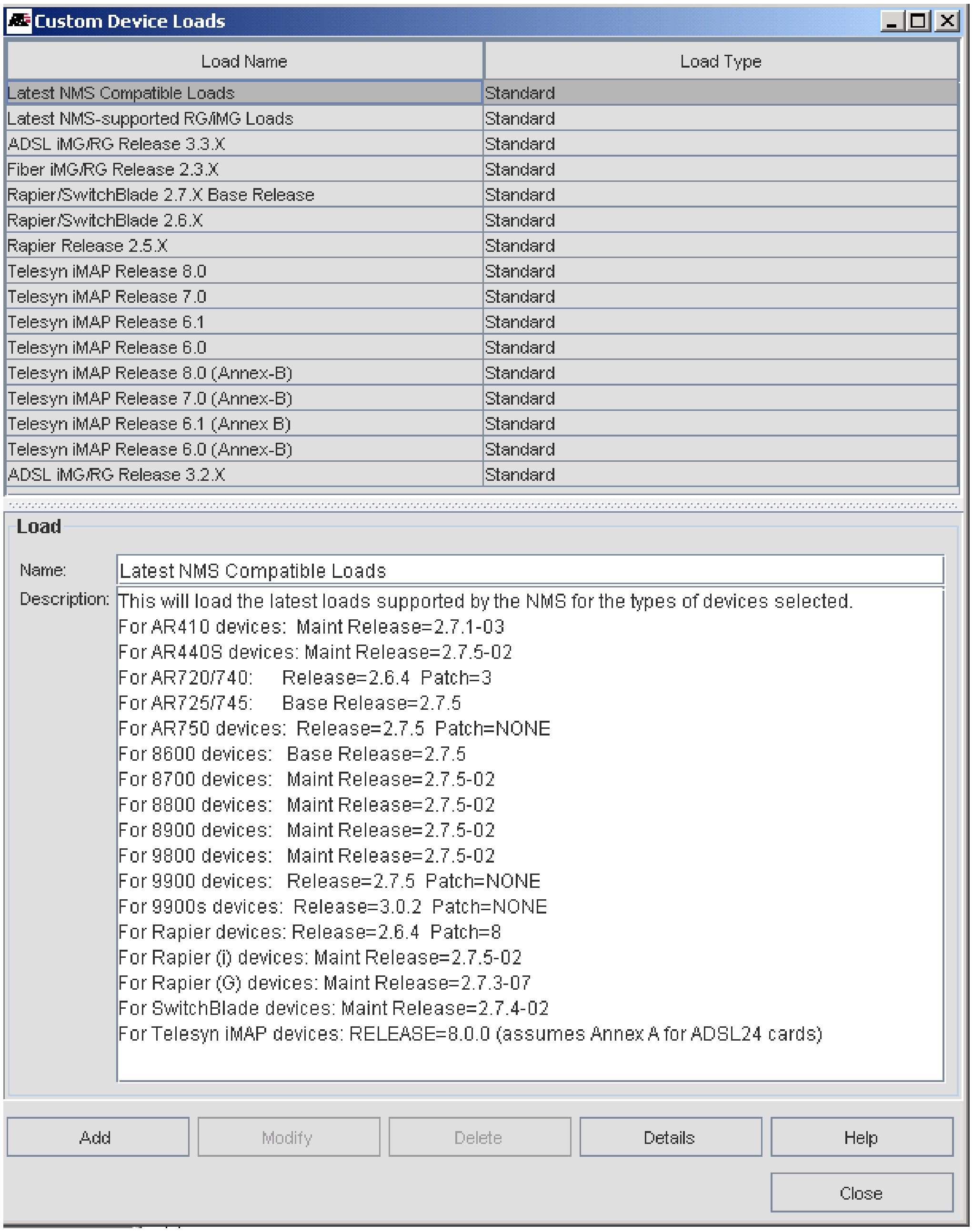
The **Delete** button allows deleting a load. Select a custom load from the table and press Delete. If the load contains any detailed data, the user will be prompted to confirm the deletion.

The **Details** button brings up the **Load Details** form for the selected load. Select a load from the table, either standard or custom, and press **Details**. Details can also be brought up by double-clicking a row. Refer to Figure 12-44.

The **Close** button closes the dialog and saves all the changes. If for any reason communication is lost to the NMS server, the user will be prompted to confirm closing (and lose any changes) or cancel closing. The message is:

Cannot Save Custom Load File. Do you want to continue exiting (and possibly lose any changes)?

After resolving the communications problem, the dialog can be closed and the data will be saved.



Load Name	Load Type
Latest NMS Compatible Loads	Standard
Latest NMS-supported RG/iMG Loads	Standard
ADSL iMG/RG Release 3.3.X	Standard
Fiber iMG/RG Release 2.3.X	Standard
Rapier/SwitchBlade 2.7.X Base Release	Standard
Rapier/SwitchBlade 2.6.X	Standard
Rapier Release 2.5.X	Standard
Telesyn iMAP Release 8.0	Standard
Telesyn iMAP Release 7.0	Standard
Telesyn iMAP Release 6.1	Standard
Telesyn iMAP Release 6.0	Standard
Telesyn iMAP Release 8.0 (Annex-B)	Standard
Telesyn iMAP Release 7.0 (Annex-B)	Standard
Telesyn iMAP Release 6.1 (Annex B)	Standard
Telesyn iMAP Release 6.0 (Annex-B)	Standard
ADSL iMG/RG Release 3.2.X	Standard

Load

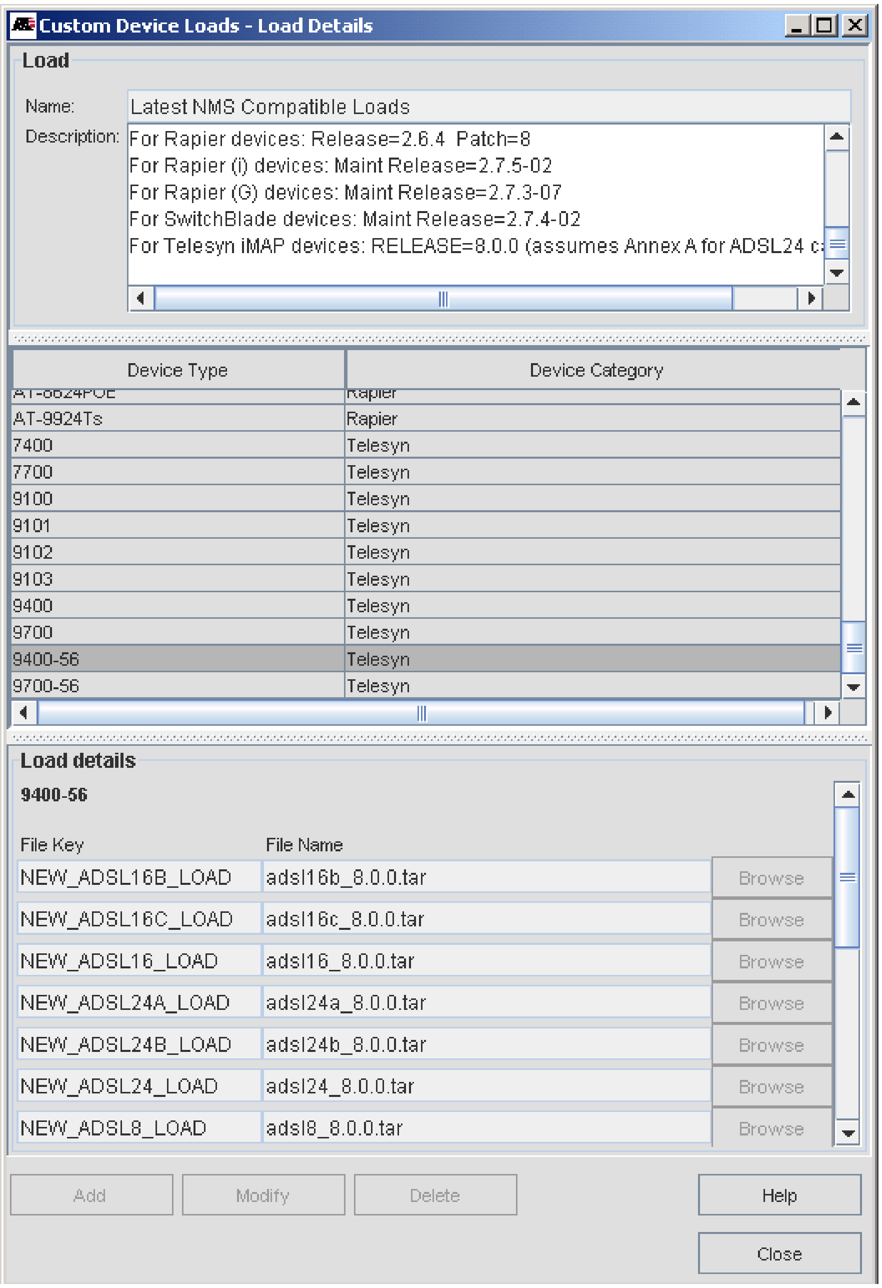
Name: Latest NMS Compatible Loads

Description:

```
This will load the latest loads supported by the NMS for the types of devices selected.
For AR410 devices:  Maint Release=2.7.1-03
For AR440S devices: Maint Release=2.7.5-02
For AR720/740:      Release=2.6.4  Patch=3
For AR725/745:      Base Release=2.7.5
For AR750 devices:  Release=2.7.5  Patch=NONE
For 8600 devices:   Base Release=2.7.5
For 8700 devices:   Maint Release=2.7.5-02
For 8800 devices:   Maint Release=2.7.5-02
For 8900 devices:   Maint Release=2.7.5-02
For 9800 devices:   Maint Release=2.7.5-02
For 9900 devices:   Release=2.7.5  Patch=NONE
For 9900s devices:  Release=3.0.2  Patch=NONE
For Rapier devices: Release=2.6.4  Patch=8
For Rapier (i) devices: Maint Release=2.7.5-02
For Rapier (G) devices: Maint Release=2.7.3-07
For SwitchBlade devices: Maint Release=2.7.4-02
For Telesyn iMAP devices: RELEASE=8.0.0 (assumes Annex A for ADSL24 cards)
```

FIGURE 12-43 Custom Device Loads Form

When the **Details** button is selected, the form is brought up, it shows the name and description of the selected load, all the types belonging to the load, and all the details for any selected type from the table. If the load is a standard load, none of the fields are modifiable. The details consist of a table of File Keys and File Names. The keys are the different types of files required to load a release and the names are the files for the particular release. In some cases, certain file types are optional and NONE will be used for the key. Refer to Figure 12-44.



Load

Name: Latest NMS Compatible Loads

Description:
For Rapier devices: Release=2.6.4 Patch=8
For Rapier (i) devices: Maint Release=2.7.5-02
For Rapier (G) devices: Maint Release=2.7.3-07
For SwitchBlade devices: Maint Release=2.7.4-02
For Telesyn iMAP devices: RELEASE=8.0.0 (assumes Annex A for ADSL24 c

Device Type	Device Category
AT-8824POE	Rapier
AT-9924Ts	Rapier
7400	Telesyn
7700	Telesyn
9100	Telesyn
9101	Telesyn
9102	Telesyn
9103	Telesyn
9400	Telesyn
9700	Telesyn
9400-56	Telesyn
9700-56	Telesyn

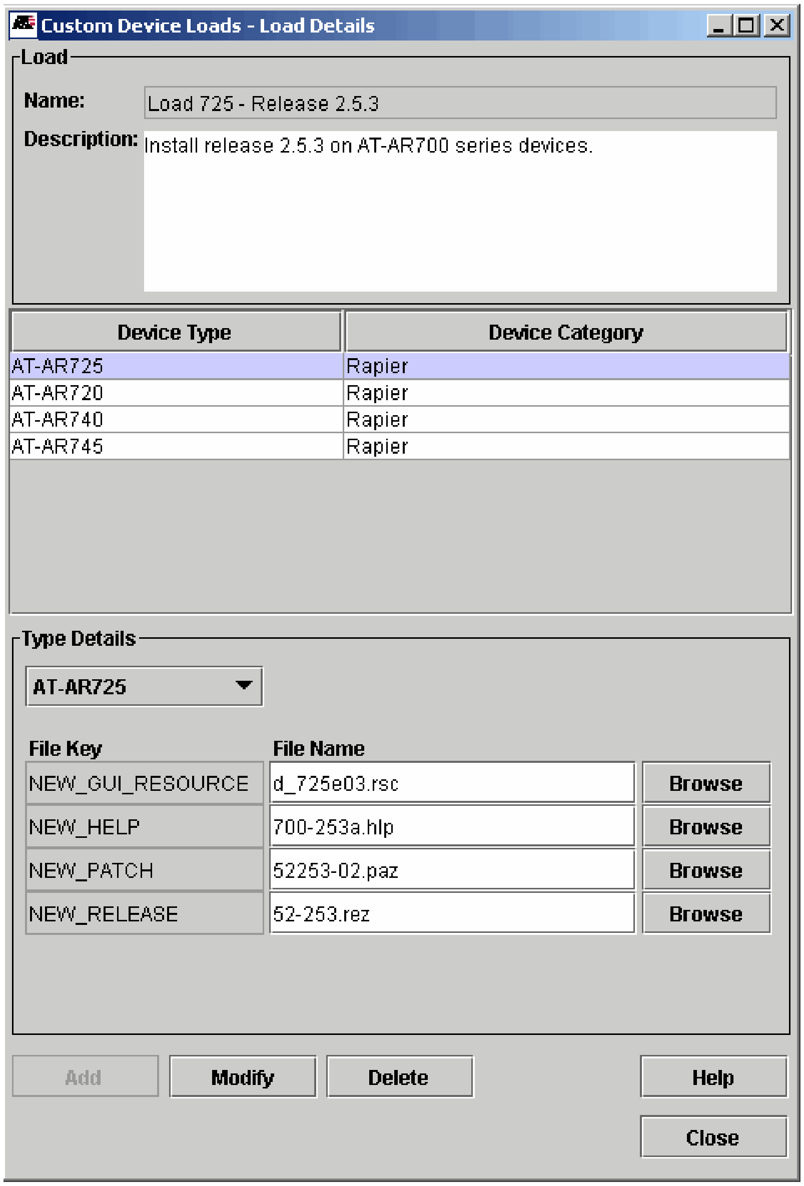
Load details

9400-56

File Key	File Name
NEW_ADSL16B_LOAD	adsl16b_8.0.0.tar
NEW_ADSL16C_LOAD	adsl16c_8.0.0.tar
NEW_ADSL16_LOAD	adsl16_8.0.0.tar
NEW_ADSL24A_LOAD	adsl24a_8.0.0.tar
NEW_ADSL24B_LOAD	adsl24b_8.0.0.tar
NEW_ADSL24_LOAD	adsl24_8.0.0.tar
NEW_ADSL8_LOAD	adsl8_8.0.0.tar

FIGURE 12-44 Custom Device Loads Form - Standard Load

If the load is a custom load, then types can be added, modified, and deleted. See Figure 12-45.



Name: Load 725 - Release 2.5.3

Description: Install release 2.5.3 on AT-AR700 series devices.

Device Type	Device Category
AT-AR725	Rapier
AT-AR720	Rapier
AT-AR740	Rapier
AT-AR745	Rapier

Type Details: AT-AR725

File Key	File Name
NEW_GUI_RESOURCE	d_725e03.rsc
NEW_HELP	700-253a.hlp
NEW_PATCH	52253-02.paz
NEW_RELEASE	52-253.rez

FIGURE 12-45 Custom Device Loads Form - Custom Load

To add a new type, begin by choosing the type from the combo box in **Type Details**, as shown in Figure 12-46. The file keys for the type are predefined and will appear in the File Keys column. The File Names will normally be blank, but in some cases where a file name was listed for the same key from the previous type, if any, the name will default to the previous name. (In some cases the same file names are usable for the same keys in different types, but in general, different device types have different keys)

If the type selected from the combo box already exists in the load, its row in the table above will be highlighted and its details will be defaulted to their existing values.

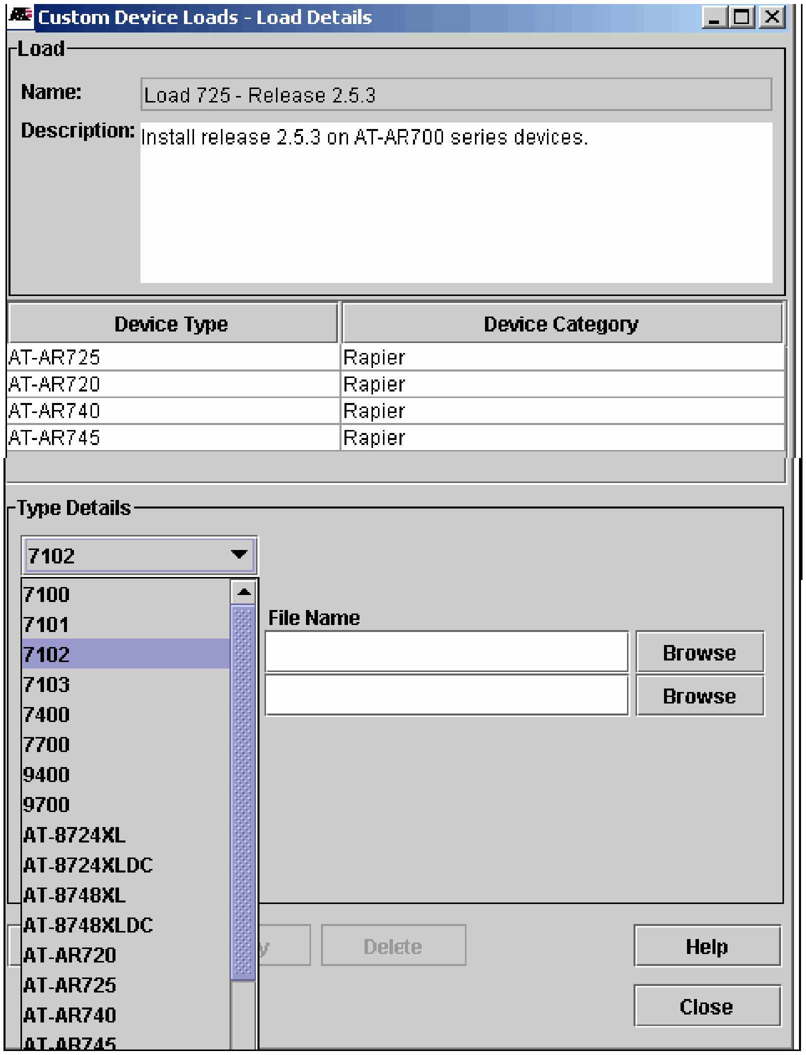
Push the **Add** button after entering all the details and verify the new type is added to the table. If you do anything else instead of pushing the Add button, a popup dialog will ask whether or not to finish the addition for the device.

The **Modify** button allows modifying the details of a type. Select the type either via the table or the combo box, modify the file names, and then push Modify. If you do anything else instead of pushing the Modify button, a popup dialog will ask whether or not to finish the modification.

The **Delete** button allows deleting a type from the load. Select the type to delete using either the combo box or the table, then push **Delete**.

More than one Details dialog can be displayed at the same time so Load contents can be compared and values can be copied and pasted from one load to another (using ctl-c and ctl-v).

Note: *Displaying details and modifying the same load in more than one simultaneous dialog, however, is not recommended. The changes to the load will occur as they're made, but all the dialogs will not be refreshed as they occur.*



Name: Load 725 - Release 2.5.3

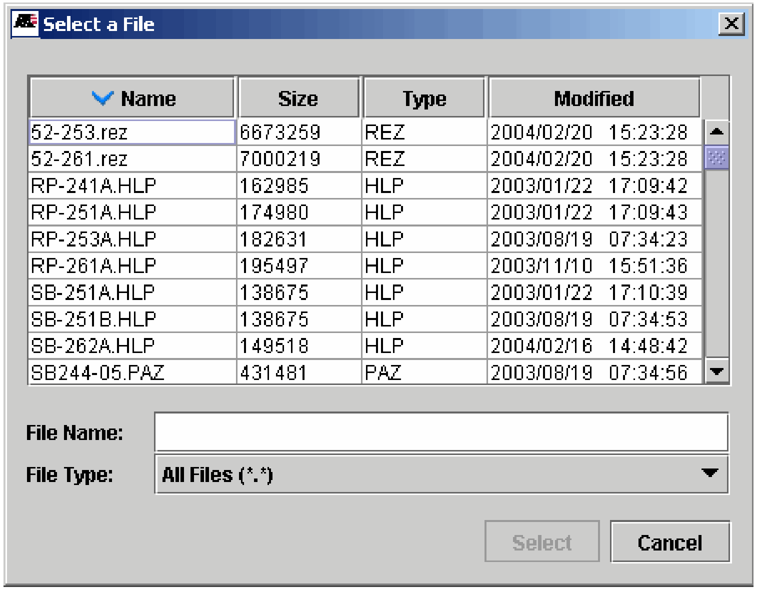
Description: Install release 2.5.3 on AT-AR700 series devices.

Device Type	Device Category
AT-AR725	Rapier
AT-AR720	Rapier
AT-AR740	Rapier
AT-AR745	Rapier

FIGURE 12-46 Load Details Form - Selecting a New Type

The file name can be typed, pasted (with ctl-v), or selected with a file chooser. The file chooser will list all the files loaded in the device's category directory (either swdownload/Rapier or swdownload/MAP). See Figure 12-47.

In some cases, one or more file names will be optional for a load. When unneeded for iMAP devices, the field should be left blank. For Rapier devices, the field should be set to NONE. Otherwise, errors may be returned during Software Configuration.



Name	Size	Type	Modified
52-253.rez	6673259	REZ	2004/02/20 15:23:28
52-261.rez	7000219	REZ	2004/02/20 15:23:28
RP-241A.HLP	162985	HLP	2003/01/22 17:09:42
RP-251A.HLP	174980	HLP	2003/01/22 17:09:43
RP-253A.HLP	182631	HLP	2003/08/19 07:34:23
RP-261A.HLP	195497	HLP	2003/11/10 15:51:36
SB-251A.HLP	138675	HLP	2003/01/22 17:10:39
SB-251B.HLP	138675	HLP	2003/08/19 07:34:53
SB-262A.HLP	149518	HLP	2004/02/16 14:48:42
SB244-05.PAZ	431481	PAZ	2003/08/19 07:34:56

File Name:

File Type: All Files (*.*)

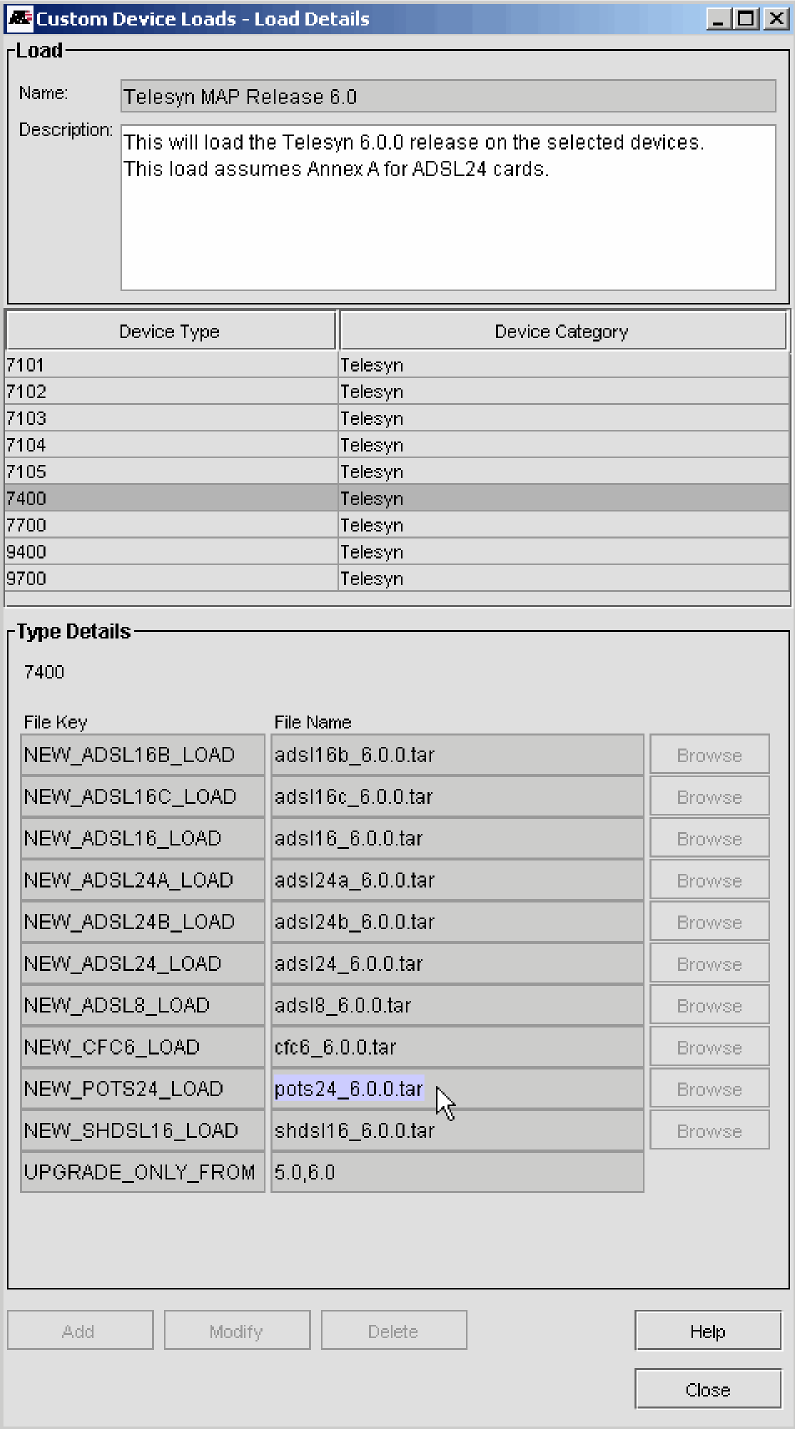
FIGURE 12-47 File Chooser - to select a file in Type Details

After creation, custom loads can be selected when modifying a device software configuration. A warning will be displayed the first time a custom load is used giving the user a last chance to back out before making sure the load configuration is defined correctly.

12.2.11 Using Custom Loads to Reduce Unneeded Card Types

Standard loads are defined to load software for all card types a device may support at a given release level. In most cases, this will be more software than necessary since most devices will not contain all possible card types. Download times and memory usage will be greater than necessary. To streamline software configuration, create a **Custom Load** containing only the necessary files. Leave the fields for the unneeded files blank. You can use the **Details** display of a standard load as a guide to see the names of the files you do need.

Figure 12-48 shows a **Load Details** window for a Standard Load that can be used as a guide for creating a streamlined Custom Load. Filenames can be copied/pasted from this display to the custom load display (Use ctl-c/ctl-v on Windows, left-click/middle-click on Linux).



Name: Telesyn MAP Release 6.0

Description: This will load the Telesyn 6.0.0 release on the selected devices.
This load assumes Annex A for ADSL24 cards.

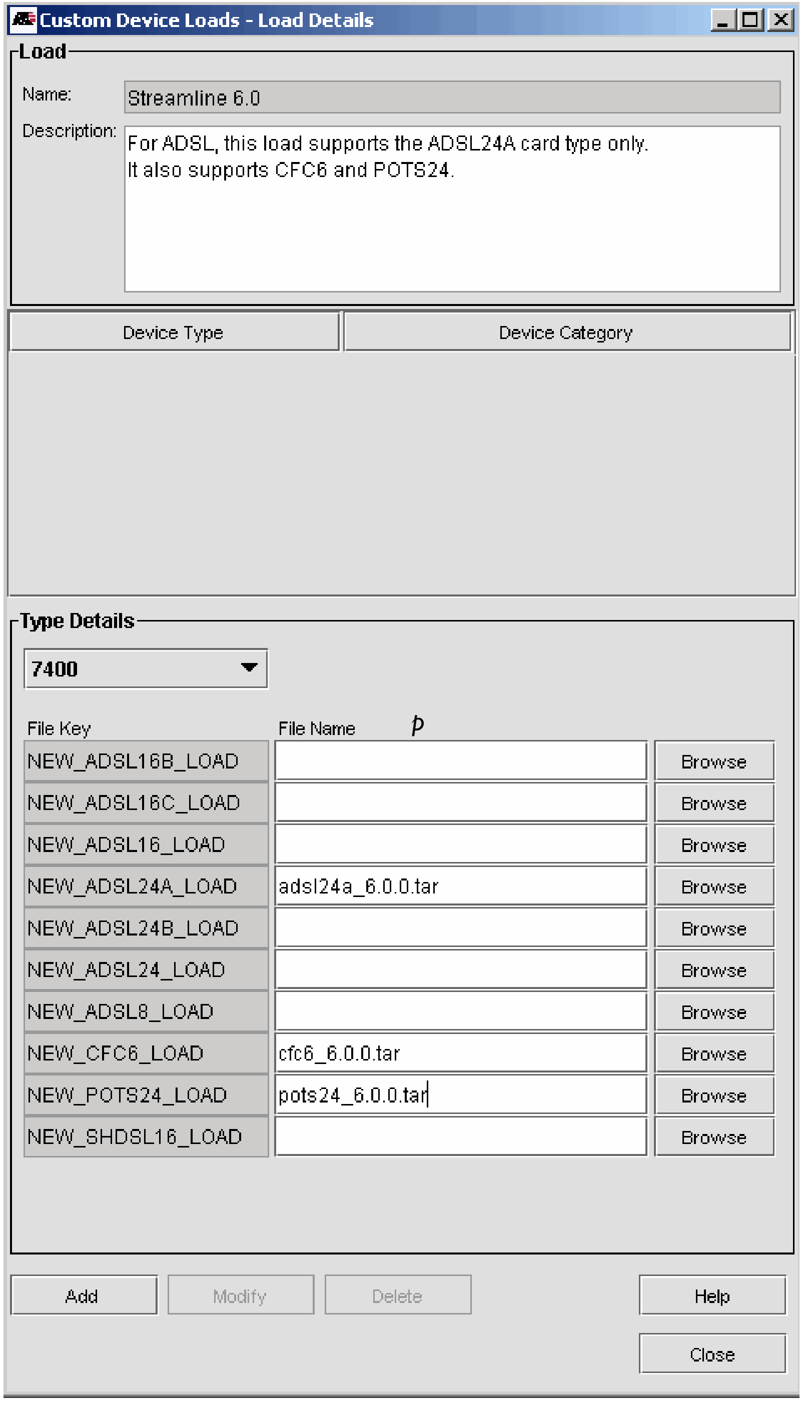
Device Type	Device Category
7101	Telesyn
7102	Telesyn
7103	Telesyn
7104	Telesyn
7105	Telesyn
7400	Telesyn
7700	Telesyn
9400	Telesyn
9700	Telesyn

7400

File Key	File Name	
NEW_ADSL16B_LOAD	adsl16b_6.0.0.tar	Browse
NEW_ADSL16C_LOAD	adsl16c_6.0.0.tar	Browse
NEW_ADSL16_LOAD	adsl16_6.0.0.tar	Browse
NEW_ADSL24A_LOAD	adsl24a_6.0.0.tar	Browse
NEW_ADSL24B_LOAD	adsl24b_6.0.0.tar	Browse
NEW_ADSL24_LOAD	adsl24_6.0.0.tar	Browse
NEW_ADSL8_LOAD	adsl8_6.0.0.tar	Browse
NEW_CFC6_LOAD	cfc6_6.0.0.tar	Browse
NEW_POTS24_LOAD	pots24_6.0.0.tar	Browse
NEW_SHDSL16_LOAD	shdsl16_6.0.0.tar	Browse
UPGRADE_ONLY_FROM	5.0,6.0	

FIGURE 12-48 Details Display for Standard Load (Used to Create Custom Load of Only Certain Files)

Figure 12-49 shows a Custom Device Loads window in which a custom load has been built that supports only the ADSL24A, CFC6, and POTS24 card types on a 7400.



Custom Device Loads - Load Details

Load

Name: Streamline 6.0

Description: For ADSL, this load supports the ADSL24A card type only.
It also supports CFC6 and POTS24.

Device Type	Device Category

Type Details

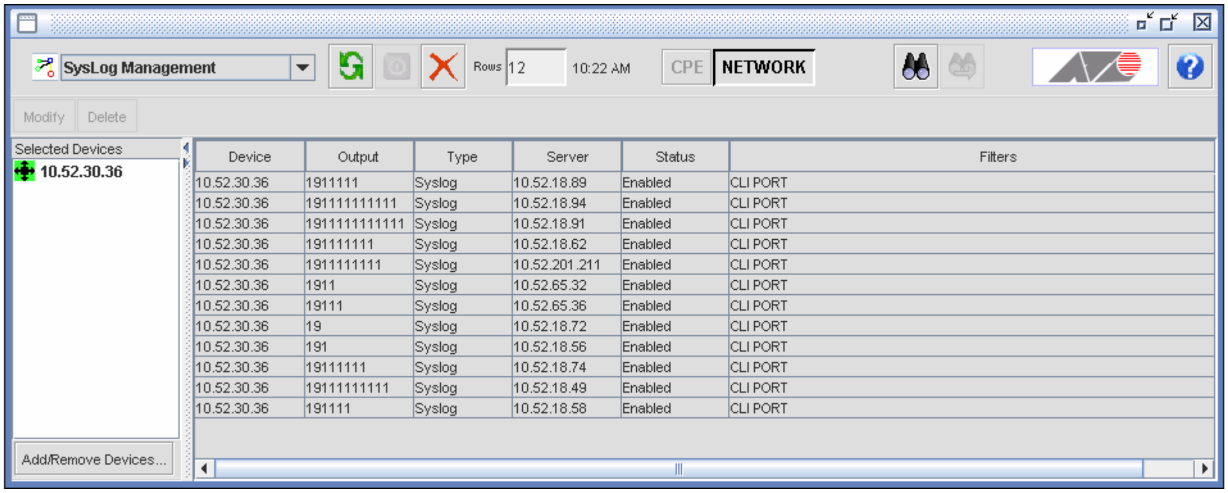
7400

File Key	File Name
NEW_ADSL16B_LOAD	
NEW_ADSL16C_LOAD	
NEW_ADSL16_LOAD	
NEW_ADSL24A_LOAD	adsl24a_6.0.0.tar
NEW_ADSL24B_LOAD	
NEW_ADSL24_LOAD	
NEW_ADSL8_LOAD	
NEW_CFC6_LOAD	cfc6_6.0.0.tar
NEW_POTS24_LOAD	pots24_6.0.0.tar
NEW_SHDSL16_LOAD	

FIGURE 12-49 Custom Load Containing Only Necessary Files

12.2.12 SysLog Management

The SysLog Management application allows you to manage logs from the managed devices in the AlliedView NMS. When the *SysLog Management* application is chosen and the **Collect Data** icon is clicked, the following figure appears.

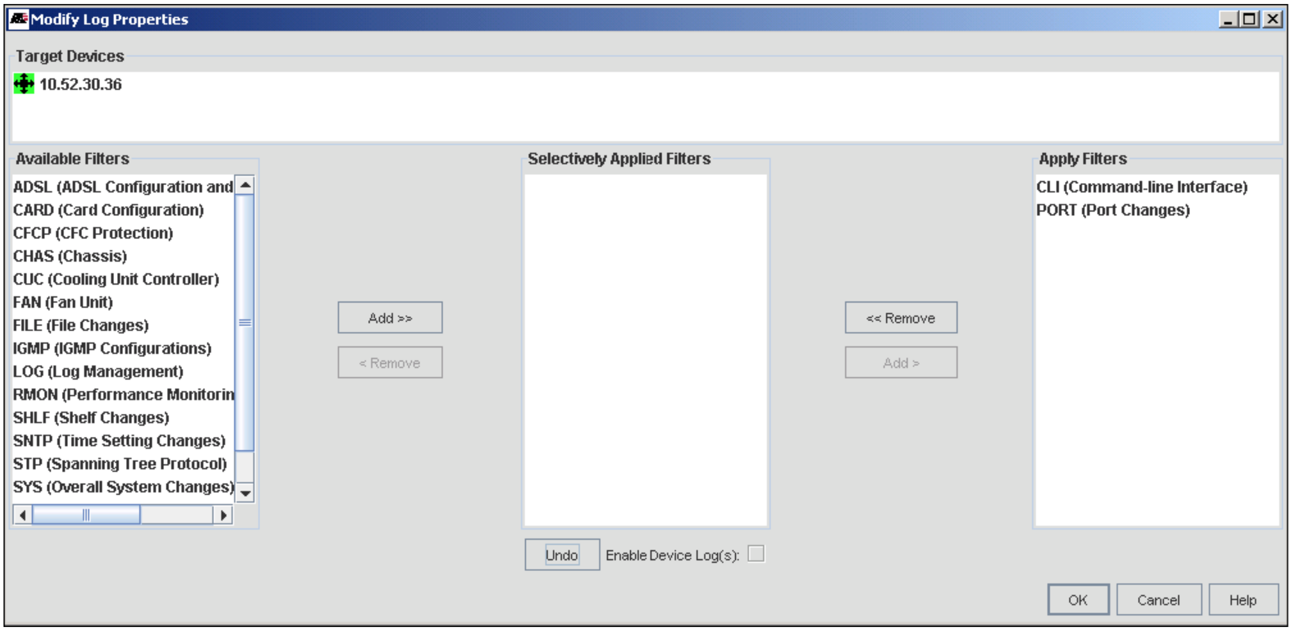


Device	Output	Type	Server	Status	Filters
10.52.30.36	1911111	Syslog	10.52.18.89	Enabled	CLI PORT
10.52.30.36	191111111111	Syslog	10.52.18.94	Enabled	CLI PORT
10.52.30.36	1911111111111	Syslog	10.52.18.91	Enabled	CLI PORT
10.52.30.36	191111111	Syslog	10.52.18.62	Enabled	CLI PORT
10.52.30.36	1911111111	Syslog	10.52.201.211	Enabled	CLI PORT
10.52.30.36	1911	Syslog	10.52.65.32	Enabled	CLI PORT
10.52.30.36	19111	Syslog	10.52.65.36	Enabled	CLI PORT
10.52.30.36	19	Syslog	10.52.18.72	Enabled	CLI PORT
10.52.30.36	191	Syslog	10.52.18.56	Enabled	CLI PORT
10.52.30.36	19111111	Syslog	10.52.18.74	Enabled	CLI PORT
10.52.30.36	19111111111	Syslog	10.52.18.49	Enabled	CLI PORT
10.52.30.36	191111	Syslog	10.52.18.58	Enabled	CLI PORT

FIGURE 12-50 SysLog Management Panel

From this panel, you can delete selected rows by pressing the **Delete** button. A confirmation window confirms the deletion.

From this panel, you can modify the system log properties of each device by selecting the device and then clicking **Modify**. When you click **Modify**, the following window appears.



Target Devices
10.52.30.36

Available Filters
ADSL (ADSL Configuration and
CARD (Card Configuration)
CFCP (CFC Protection)
CHAS (Chassis)
CUC (Cooling Unit Controller)
FAN (Fan Unit)
FILE (File Changes)
IGMP (IGMP Configurations)
LOG (Log Management)
RMON (Performance Monitorin
SHLF (Shelf Changes)
SNTP (Time Setting Changes)
STP (Spanning Tree Protocol)
SYS (Overall System Changes)

Selectively Applied Filters

Apply Filters
CLI (Command-line Interface)
PORT (Port Changes)

Enable Device Log(s): □

FIGURE 12-51 SysLog Management Application Modify Log Properties Window - File

This window allows you to apply or remove system log filters to or from each device. The **Available Filters** list box lists the log filters that may be applied to the selected devices. The **Selectively Applied Filters** list box lists filters that are applied to some of the selected devices, but not all. The **Apply Filters** list box lists the filters that are applied to all of the selected devices.

For information on configuring the AlliedView NMS system logs, refer to "Configuring System Logs" on page 1017.

12.2.13 LLDP Protocol and Associated Features (LAG/VCS Monitoring)

The LLDP protocol feature on devices is a way to advertise data that is useful for discovering information about a network link port. If the administrator manually enables LLDP for each device and sets the direction as BOTH, the links between the devices will appear on the physical map GUI as the devices are (re)discovered.

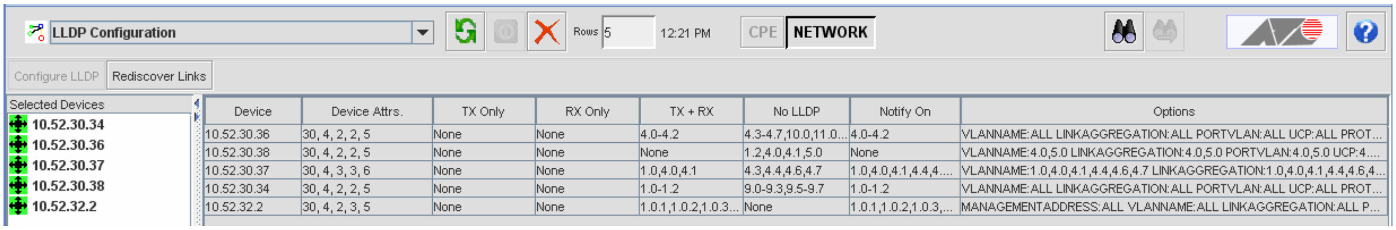
Note: For a complete description of LLDP and its parameters, refer to the Software Reference for iMAP Series Switches.

The administrator can activate and control LLDP for one or multiple devices using an application. Moreover, one minute after LLDP has been activated (with a direction of BOTH), the device will be re-discovered and the links will appear on the physical map based on the LLDP data.

Caution: It is not recommended to include a HUB switch when using the LAG/VCS monitoring feature or any feature that uses the LLDP application. A HUB switch provides a one-to-many configuration for data traffic, so all LLDP information is propagated to multiple devices. As a result, the devices will build an incorrect set of connection information. Moreover, the topology displayed will not be correct, and can even look like a loop.

Like other applications, the administrator can select one or more devices, right click, and then choose *Provision -> LLDP Configuration*, and then bring up the application, as shown in the following figure.

Note: You can also select Tools -> Application Manager, select LLDP Configuration in the pull-down menu, and add devices.



Device	Device Attrs.	TX Only	RX Only	TX + RX	No LLDP	Notify On	Options
10.52.30.36	30, 4, 2, 2, 5	None	None	4.0-4.2	4.3-4.7,10.0,11.0...	4.0-4.2	VLANNAME:ALL LINKAGGREGATION:ALL PORTVLAN:ALL UCP:ALL PROT...
10.52.30.38	30, 4, 2, 2, 5	None	None	None	1.2,4.0,4.1,5.0	None	VLANNAME:4.0,5.0 LINKAGGREGATION:4.0,5.0 PORTVLAN:4.0,5.0 UCP:4....
10.52.30.37	30, 4, 3, 3, 6	None	None	1.0,4.0,4.1	4.3,4.4,4.6,4.7	1.0,4.0,4.1,4.4,4....	VLANNAME:1.0,4.0,4.1,4.4,4.6,4.7 LINKAGGREGATION:1.0,4.0,4.1,4.4,4.6,4...
10.52.30.34	30, 4, 2, 2, 5	None	None	1.0-1.2	9.0-9.3,9.5-9.7	1.0-1.2	VLANNAME:ALL LINKAGGREGATION:ALL PORTVLAN:ALL UCP:ALL PROT...
10.52.32.2	30, 4, 2, 3, 5	None	None	1.0.1,1.0.2,1.0.3...	None	1.0.1,1.0.2,1.0.3,...	MANAGEMENTADDRESS:ALL VLANNAME:ALL LINKAGGREGATION:ALL P...

FIGURE 12-52 LLDP Application for iMAP Devices

The application shows for each device the following:

- Device Attrs. - These are listed and allowed to be changed in the first **LLDP MultiDevice Wizard** panel.
- Direction - This can be TX, RX or both.
- No LLDP - Whether LLDP is active or not on the port. (This is controlled by the Notify option.)

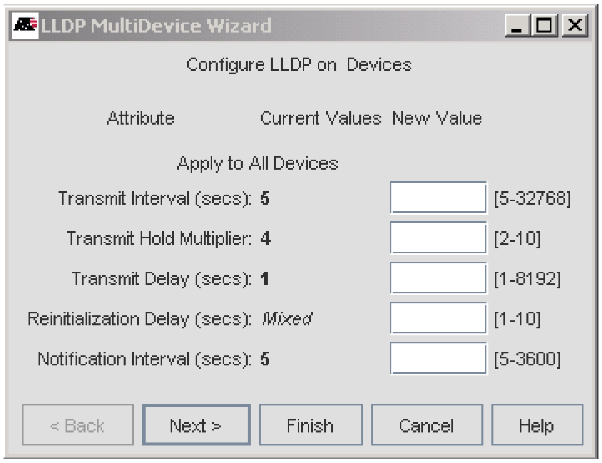
Options - There are multiple options, and these are controlled by the second **LLDP MultiDevice Wizard** panel.

The administrator can choose one or multiple devices with which to activate and control LLDP, as explained below.

12.2.13.1 LLDP for Multiple Devices

Note: In most cases, the administrator should first choose all the relevant devices that will have LLDP activated and set the attributes for all devices. The administrator could then if desired choose a device and change specific attributes. Otherwise, if settings are applied to a specific device, and changes are then made for multiple devices that affect those settings, any changes to that specific device would be overwritten.

When more than one device is chosen and the **Configure LLDP** Button is selected, the **LLDP MultiDevice Wizard** panel appears. The following figure shows the first panel when multiple devices are selected.



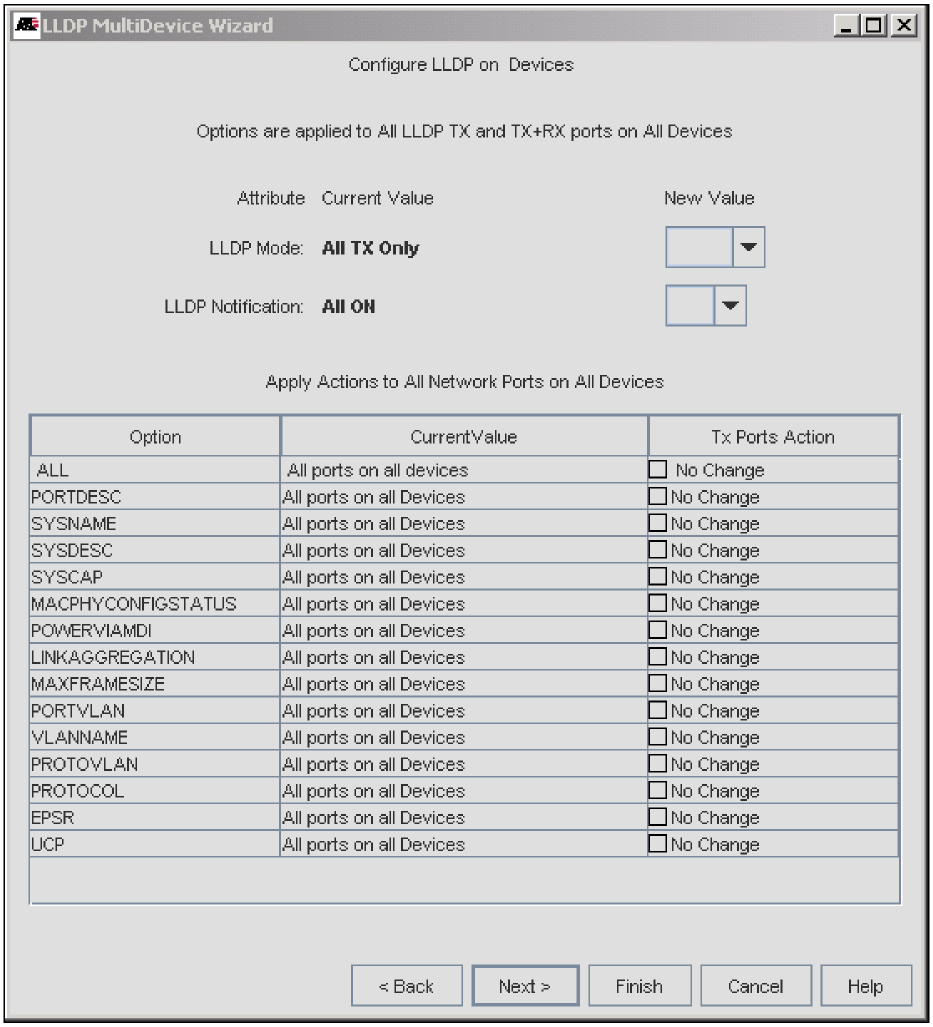
Configure LLDP on Devices

Attribute	Current Values	New Value	
Apply to All Devices			
Transmit Interval (secs):	**5**		[5-32768]
Transmit Hold Multiplier:	**4**		[2-10]
Transmit Delay (secs):	**1**		[1-8192]
Reinitialization Delay (secs):	*Mixed*		[1-10]
Notification Interval (secs):	**5**		[5-3600]

FIGURE 12-53 LLDP MultiDevice Wizard for Multiple iMAP Devices - First Panel

Note the Re initialization Delay attribute has *Mixed* rather than a numeric value. This means there are different values of the devices. Inputting a New Value (such as 2) will change the value to 2 for **all** the selected devices.

The second panel brings up a panel that controls the options for the multiple devices. The following figure shows an example where LLDP is set to All OFF.



Configure LLDP on Devices

Options are applied to All LLDP TX and TX+RX ports on All Devices

Attribute	Current Value	New Value
LLDP Mode:	All TX Only	
LLDP Notification:	All ON	

Apply Actions to All Network Ports on All Devices

Option	CurrentValue	Tx Ports Action
ALL	All ports on all devices	□ No Change
PORTDESC	All ports on all Devices	□ No Change
SYSNAME	All ports on all Devices	□ No Change
SYSDESC	All ports on all Devices	□ No Change
SYSCAP	All ports on all Devices	□ No Change
MACPHYCONFIGSTATUS	All ports on all Devices	□ No Change
POWERVIAMDI	All ports on all Devices	□ No Change
LINKAGGREGATION	All ports on all Devices	□ No Change
MAXFRAMESIZE	All ports on all Devices	□ No Change
PORTVLAN	All ports on all Devices	□ No Change
VLANNAME	All ports on all Devices	□ No Change
PROTOVLAN	All ports on all Devices	□ No Change
PROTOCOL	All ports on all Devices	□ No Change
EPSR	All ports on all Devices	□ No Change
UCP	All ports on all Devices	□ No Change

FIGURE 12-54 LLDP MultiDevice Wizard for Multiple iMAP Devices - Second Panel

The pull-downs are as follows:

- LLDP Mode - The options are TX, RX, BOTH or OFF. Note that **to activate LLDP so that the links are drawn on the physical map, this must be set to BOTH**. The specific attributes for the ports can then be set.
- LLDP Notification - This can be set to ON or OFF.

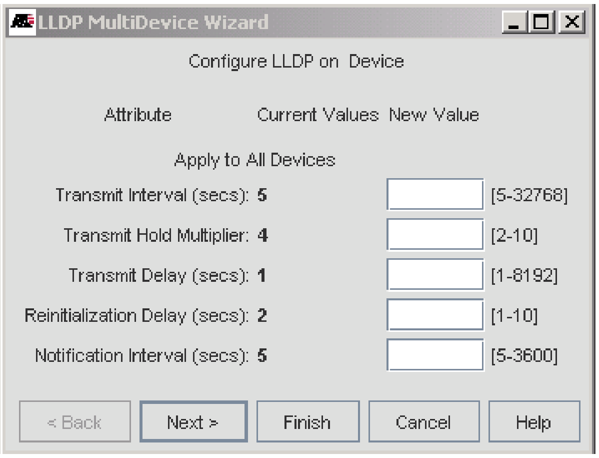
For the options, the Current Value shows how the option is currently being applied. The user has the following actions to choose from:

- ALL Row
  - Add to All - make all options apply to all ports if the option is not applied to any or some ports
  - Delete from All - delete all options from all ports if the option is applied to any or some ports.
- Other options
  - Add to All - make the one option apply to all ports. This would take priority over the ALL Row.
  - Delete from All - make the one option be deleted for all ports. This would take priority over the ALL Row.
  - No Change - Keep the current value regardless of any changes made with the ALL option. This would only apply if the current value was not All ports on All devices.

The user can then select **Finish** to bring up the Task Details window or **Next** to bring up the Task Schedule wondow.

12.2.13.2 LLDP for One Device

When the **Configure LLDP** button is activated, and when pressed the first **LLDP MultiDevice Wizard** panel appears, as shown in the following figure.



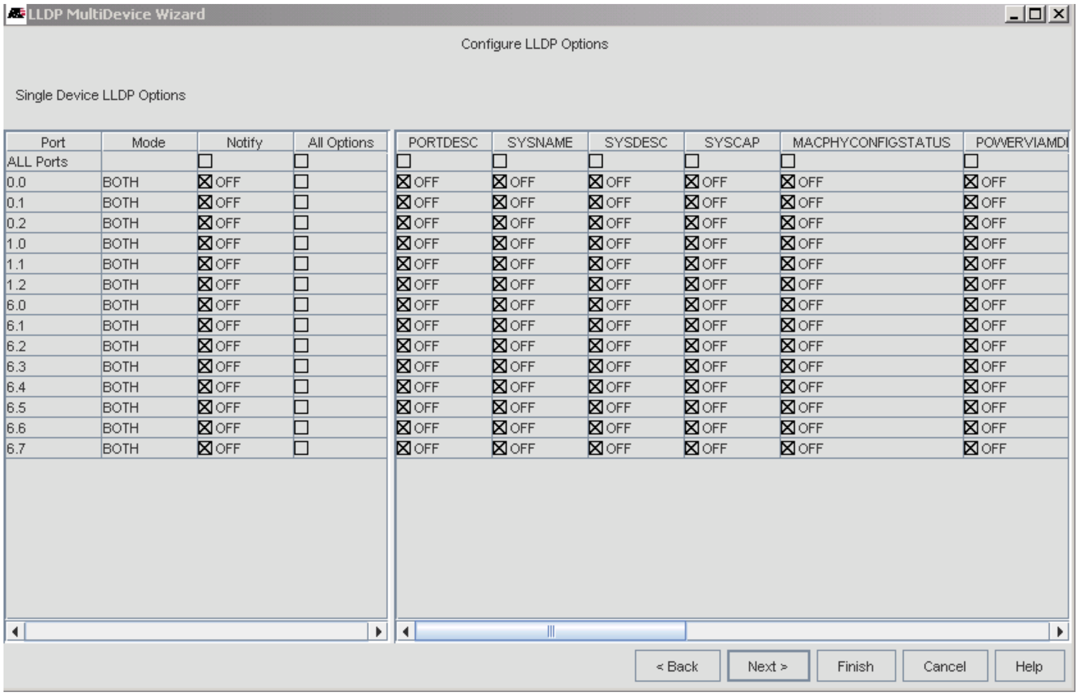
LLDP MultiDevice Wizard

Configure LLDP on Device

Attribute	Current Values	New Value	
Apply to All Devices			
Transmit Interval (secs):	**5**		[5-32768]
Transmit Hold Multiplier:	**4**		[2-10]
Transmit Delay (secs):	**1**		[1-8192]
Reinitialization Delay (secs):	**2**		[1-10]
Notification Interval (secs):	**5**		[5-3600]

FIGURE 12-55 LLDP MultiDevice Wizard for One iMAP Device - First Panel

The current values for the selected device is shown, and the user can change the values within the range shown. Selecting the **Finish** button brings up the Task Window to show the progress of the changes taking effect. Selecting the **Next** button brings up the Configure LLDP Options panel, as shown in the following figure.



LLDP MultiDevice Wizard

Configure LLDP Options

Single Device LLDP Options

Port	Mode	Notify	All Options
ALL Ports		□	□
0.0	BOTH	☒ OFF	□
0.1	BOTH	☒ OFF	□
0.2	BOTH	☒ OFF	□
1.0	BOTH	☒ OFF	□
1.1	BOTH	☒ OFF	□
1.2	BOTH	☒ OFF	□
6.0	BOTH	☒ OFF	□
6.1	BOTH	☒ OFF	□
6.2	BOTH	☒ OFF	□
6.3	BOTH	☒ OFF	□
6.4	BOTH	☒ OFF	□
6.5	BOTH	☒ OFF	□
6.6	BOTH	☒ OFF	□
6.7	BOTH	☒ OFF	□

PORTDESC	SYSNAME	SYSDESC	SYSCAP	MACPHYCONFIGSTATUS	POWERVIAMDI
□	□	□	□	□	□
☒ OFF	☒ OFF	☒ OFF	☒ OFF	☒ OFF	☒ OFF
☒ OFF	☒ OFF	☒ OFF	☒ OFF	☒ OFF	☒ OFF
☒ OFF	☒ OFF	☒ OFF	☒ OFF	☒ OFF	☒ OFF
☒ OFF	☒ OFF	☒ OFF	☒ OFF	☒ OFF	☒ OFF
☒ OFF	☒ OFF	☒ OFF	☒ OFF	☒ OFF	☒ OFF
☒ OFF	☒ OFF	☒ OFF	☒ OFF	☒ OFF	☒ OFF
☒ OFF	☒ OFF	☒ OFF	☒ OFF	☒ OFF	☒ OFF
☒ OFF	☒ OFF	☒ OFF	☒ OFF	☒ OFF	☒ OFF
☒ OFF	☒ OFF	☒ OFF	☒ OFF	☒ OFF	☒ OFF
☒ OFF	☒ OFF	☒ OFF	☒ OFF	☒ OFF	☒ OFF
☒ OFF	☒ OFF	☒ OFF	☒ OFF	☒ OFF	☒ OFF
☒ OFF	☒ OFF	☒ OFF	☒ OFF	☒ OFF	☒ OFF
☒ OFF	☒ OFF	☒ OFF	☒ OFF	☒ OFF	☒ OFF
☒ OFF	☒ OFF	☒ OFF	☒ OFF	☒ OFF	☒ OFF

FIGURE 12-56 LLDP MultiDevice Wizard for Single Device Options - Second Panel

To configure the many possible options, the following concepts are used:

- ALL Ports row - This row controls multiple actions as follows:

- **Mode** - Selecting this cell brings up a pull-down of Modes, and selecting one means selecting the Mode for all ports on the device, including OFF, which disables LLDP for all ports.
- **Notify** - Selecting this tic box toggles the Notify option for all ports between All On (with all ports in the column having the tic boxes checked) and All Off (with all tic boxes in the column blank).
- **All options** - This allows the user to add all options to all ports or delete all options from all ports.
- Specific option - For each option, selecting the tic box will Add or Delete the option for all ports.

- Row for each port - This row controls the options for each port as follows:
  - **Mode** - Selecting this cell brings up a pull-down of Modes, and selecting one means selecting the Mode for only that specific port.
  - **Notify** - Selecting this tic box toggles the Notify option on the port between ON and Disable.
  - **All options** - This tic box controls the state of all the options on the port
  - Specific Option - selects the specific option for the specific port.

Note: Setting any specific option for a will override a global options.

The user can then select **Finish** to bring up the Task Details window or **Next** to bring up the Task Schedule window.

12.2.13.3 LAG and VCS Support

The Physical Network Map shows the discovered devices and the physical connections (links) between them. The physical link icon between devices appears if the both devices support LLDP, and the NMS actively supports the LLDP functionality of the device.

Note: The physical links can also be manually created using the Link Operation function. Refer to "Physical Network Map" on page 527.

On this Map, there is a feature that shows the LAG and Virtual Chassis Stacking (VCS) configuration.

- Stacked Devices - If a device is discovered to be set in a stacked configuration, its node will be rendered as two node icons stacked on top of each other, regardless of how many units comprise the stack. Moreover, the outline of the bottom icon is rendered blue if the stack is functioning normally, and orange if one or more members of the stack is unavailable. Refer to the following figure.

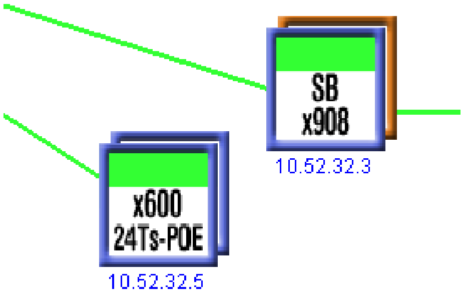


FIGURE 12-57 Icons for Stacked Devices - SBx908 has member of stack unavailable

- LAG - If two or more links are aggregated, forming a LAG connection, the LAG link is rendered as two parallel lines. Moreover, if both links are rendered as green, all links are available. If one of the two links is orange, then:
  - One or more links of the LAG is unavailable.
  - The neighboring port is not configured for LAG.
  - (AlliedWare type devices) - The port is not associated to any LACP channel.

  Refer to the following figure.

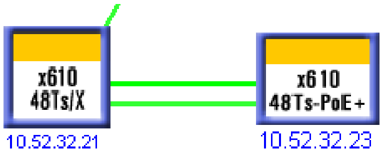
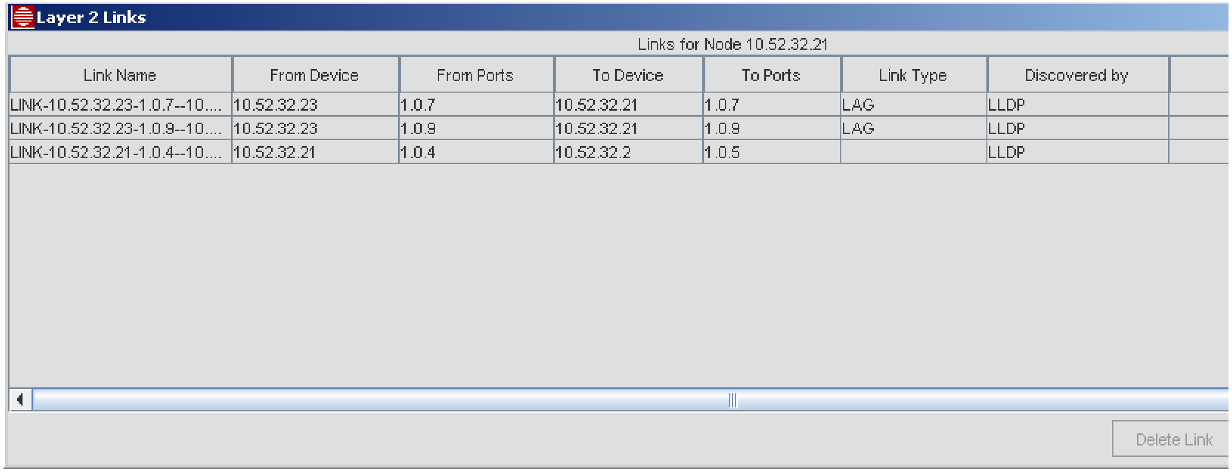


FIGURE 12-58 Icons for LAG links

- Layer 2 Links Screen - This screen shows the attributes of the links for the device and allows the user to create and add links. (You can access the this screen by right clicking on a device and selecting *Network Services -> Link Operations*.) The Link Type indicates LAG, as shown the following figure.



Links for Node 10.52.32.21

Link Name	From Device	From Ports	To Device	To Ports	Link Type	Discovered by
LINK-10.52.32.23-1.0.7--10....	10.52.32.23	1.0.7	10.52.32.21	1.0.7	LAG	LLDP
LINK-10.52.32.23-1.0.9--10....	10.52.32.23	1.0.9	10.52.32.21	1.0.9	LAG	LLDP
LINK-10.52.32.21-1.0.4--10....	10.52.32.21	1.0.4	10.52.32.2	1.0.5		LLDP

FIGURE 12-59

- **Show LAG Links** option - Right click on the LAG links icon and select **Show LAG Links** to bring up the LAG/VCS screen. Refer to the following figure.

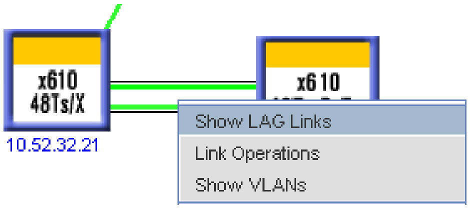


FIGURE 12-60 Accessing the Show LAG Links Screen

- LAG/VCS screen - This shows details such as the number of links that make up a LAG, the status of each LAG member, the port ID and LAG ID of each link, and, if VCS is configured as well, which stack member a LAG member is connected to. It also shows the endpoints, which can be non-stacked or stacked. Non-stacked endpoints have the same icon as for devices in the Physical Network Map. Stacked endpoints are shown as a stacked node, with each node representing a stack member. (Members are sorted from lowest to highest ID.) Finally, each link of the LAG is shown, where a link that is UP is green, and a link that is down or unavailable is shown as orange. Refer to the following figure.

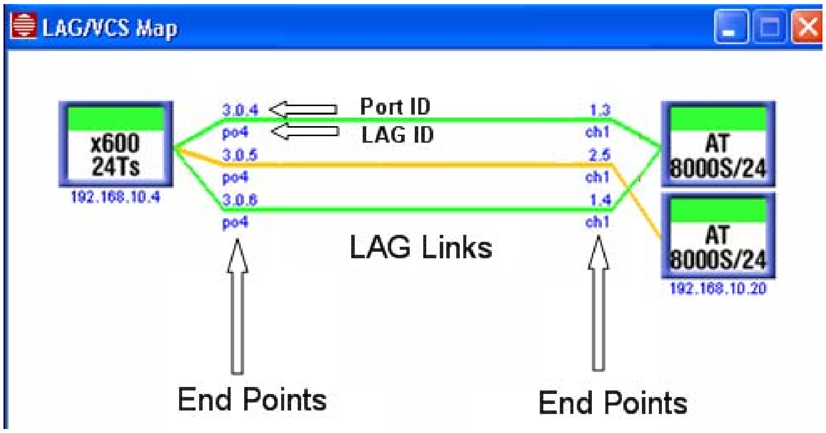


FIGURE 12-61 LAG/VCS Map Screen

The LAG ID can be as follows:

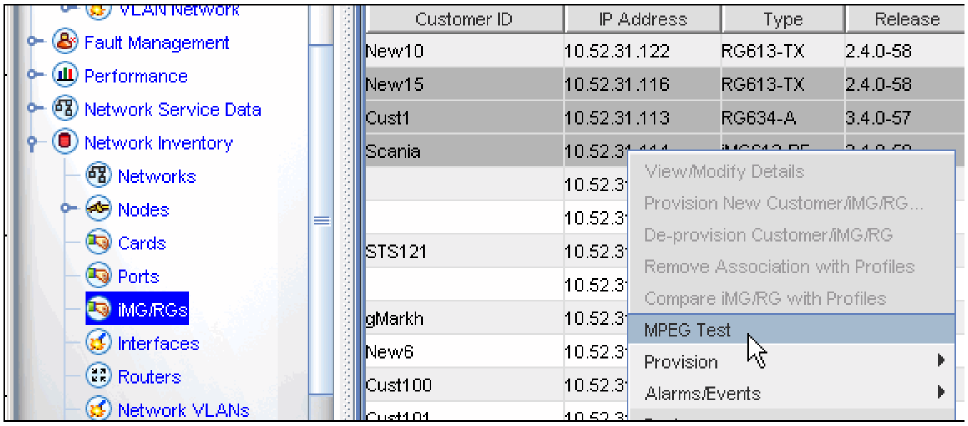
- **<LAG ID>** - Port is not down and LAG channel is up
- **Not Configured** - Port is not configured for LAG but the neighboring port is
- **-** (AlliedWare devices) - Port is not associated with any LAG Channel

- Chassis View - In the Chassis View for a device, ports that are members of a LAG are labeled “LA”. Note that the state of these ports cannot be changed (cannot change the state from <blank> -> T -< U).

12.2.14 MPEG Test

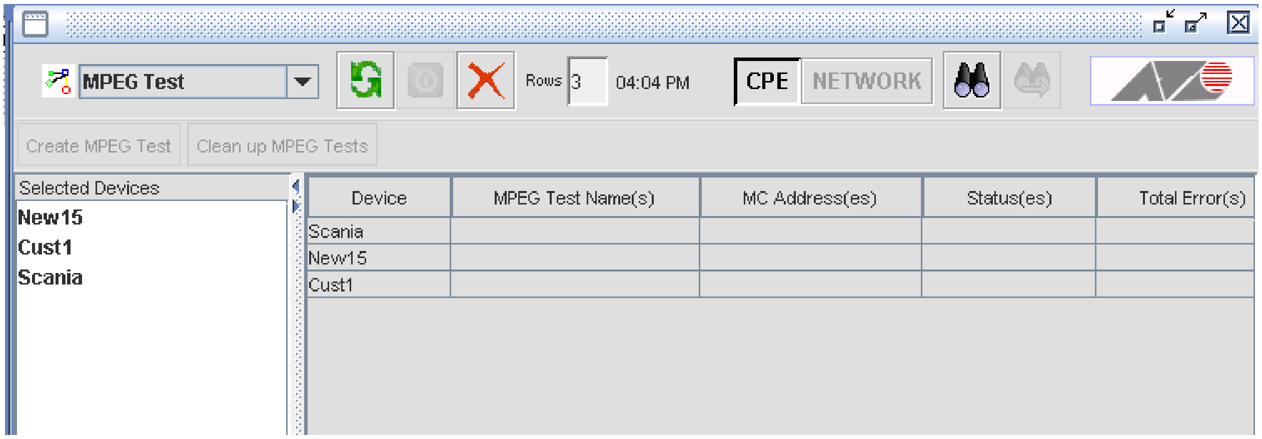
The MPEG Test feature allows the user to setup, monitor, and view the results of MPEG tests run on the iMG/RGs in a network. With the feature the user can set up a “Network Test” across multiple iMGs in a network. Once set up, the NMS runs an MPEG test on the selected iMGs using the mpeg testing functionality included with the iMGs devices. The the NMS collects the results of those tests and stores them in the NMS database, where they can be viewed. (Note that once a day test results are deleted that is older than seven days.)

To access the feature, the user accesses the application as described in "Overview of the Provisioning Interface" on page 275. The user can also go to Network Inventory, select the RG table, choose the appropriate iMGs, right click, and select MPEG Test from the pull-down. Refer to the following figures.



Customer ID	IP Address	Type	Release
New10	10.52.31.122	RG613-TX	2.4.0-58
New15	10.52.31.116	RG613-TX	2.4.0-58
Cust1	10.52.31.113	RG634-A	3.4.0-57
Scania	10.52.31		
	10.52.3		
	10.52.3		
STS121	10.52.3		
	10.52.3		
gMarkh	10.52.3		
New6	10.52.3		
Cust100	10.52.3		

FIGURE 12-62 Example Method to Access MPEG Test Feature

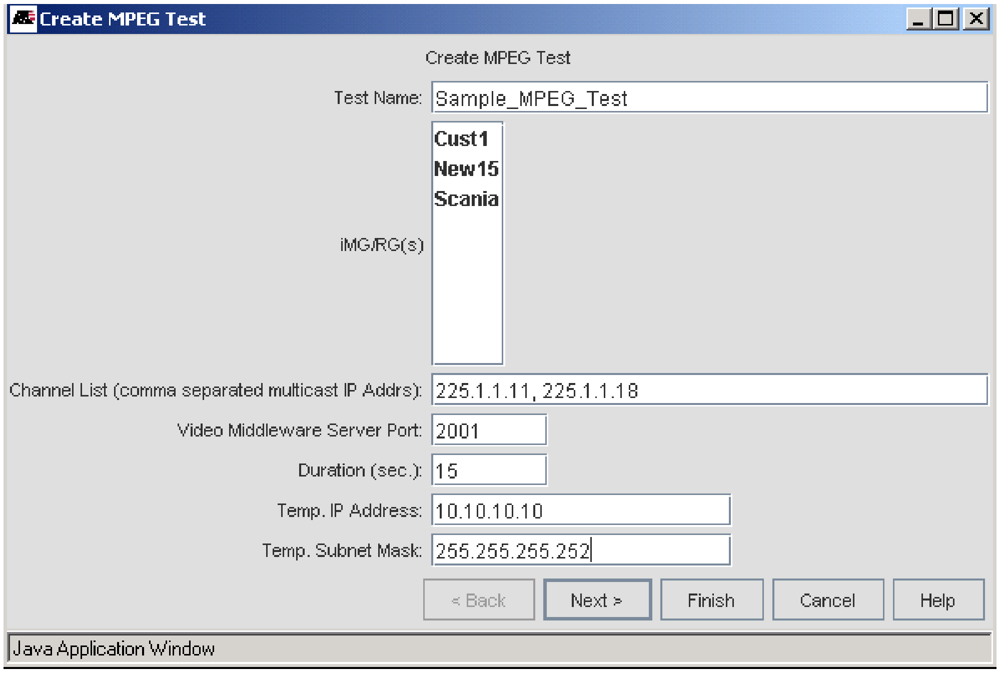


Selected Devices
New15
Cust1
Scania

Device	MPEG Test Name(s)	MC Address(es)	Status(es)	Total Error(s)
Scania				
New15				
Cust1				

FIGURE 12-63 Initial GUI for MPEG Test Feature

To start the test, the user selects a set of iMG/RGs from the table and selects the now active “Create MPEG Test” button. This brings up the Create MPEG Test Form, shown in the following figure.



Create MPEG Test

Create MPEG Test

Test Name: Sample_MPEG_Test

iMG/RG(s): Cust1, New15, Scania

Channel List (comma separated multicast IP Addrs): 225.1.1.11, 225.1.1.18

Video Middleware Server Port: 2001

Duration (sec.): 15

Temp. IP Address: 10.10.10.10

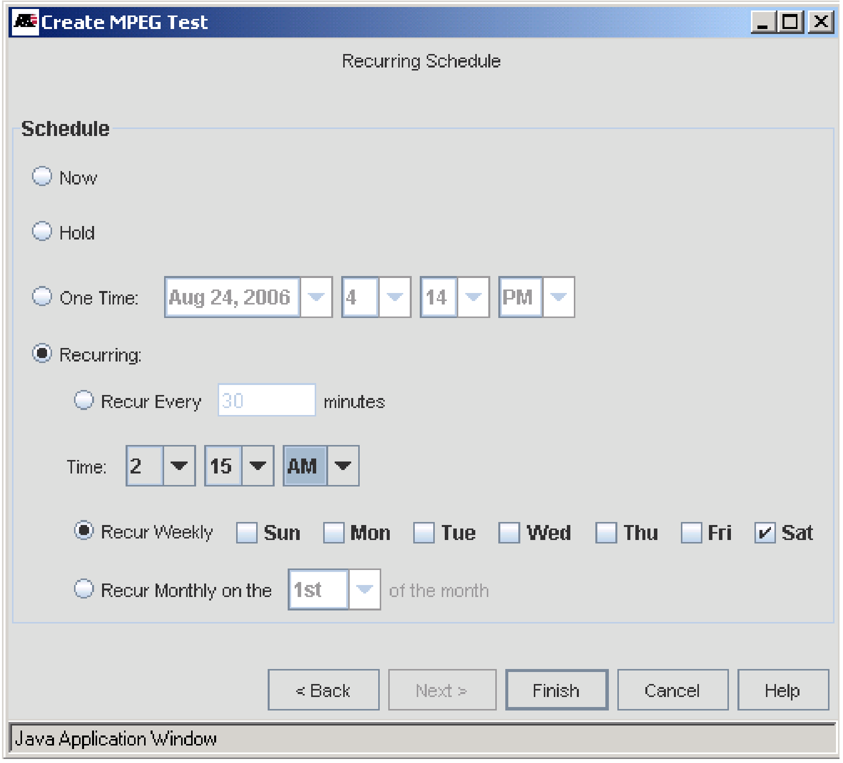
Temp. Subnet Mask: 255.255.255.252

FIGURE 12-64 Create MPEG Test Form

Fields to datafill are:

- Test Name - This should be descriptive, and becomes the Name of the test in the Task List Details window.
- Channel List - The multicast IP address(es) for the channel(s) to be tested. If multiple channels are entered, each channel will be tested sequentially. (If multiple iMG/RGs were selected, all iMG/RGs will be tested simultaneously.) Example values would be 225.1.1.11, 225.1.1.18
- Video Middleware Server Port - The port of the video server to be used, such as 2001.
- Duration - Length the test will run, in seconds
- Temp. IP Address - The default is 10.0.0.254
- Temp Subnet IP Address - The default is 255.255.255.252

Selecting Finish starts the test immediately, or the user can select Next to create a schedule, as shown in the following figure.



Create MPEG Test

Recurring Schedule

Schedule

○ Now

○ Hold

○ One Time: Aug 24, 2006 4 14 PM

● Recurring:

○ Recur Every 30 minutes

Time: 2 15 AM

● Recur Weekly □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri ☑ Sat

○ Recur Monthly on the 1st of the month

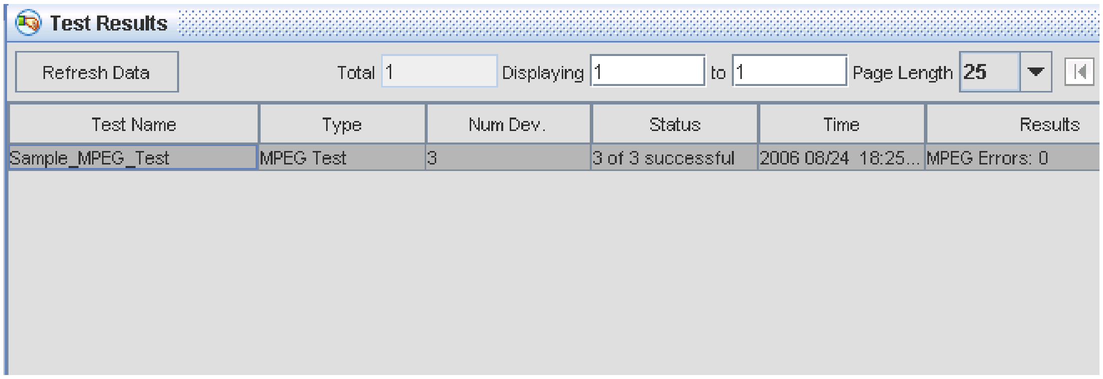
FIGURE 12-65 Create MPEG Test - Recurring Schedule

For the recurring schedule, the user can choose:

- Now - Click Finish to start the test immediately.
- Hold - This sets no time; the test is activated through the View Tasks window.
- One Time - Sets one time only to run the test
- Recurring - This is set on a minute basis and can be one time, a specific time every week (shown in the above figure), or a specific time on a day of the month. (Selecting 29-31 of month means those months that do not have those numbered days will skip the test for that month.)

As with other applications, once the test is created, the user can view the parameters and the schedule of the test by bringing up the “View Tasks” window, selecting a MPEG Test task, and pressing the “View Details” button.

To access the results of the test, open the Network Service Data leaf in the main tree and select Test Results, as shown in the following figure.

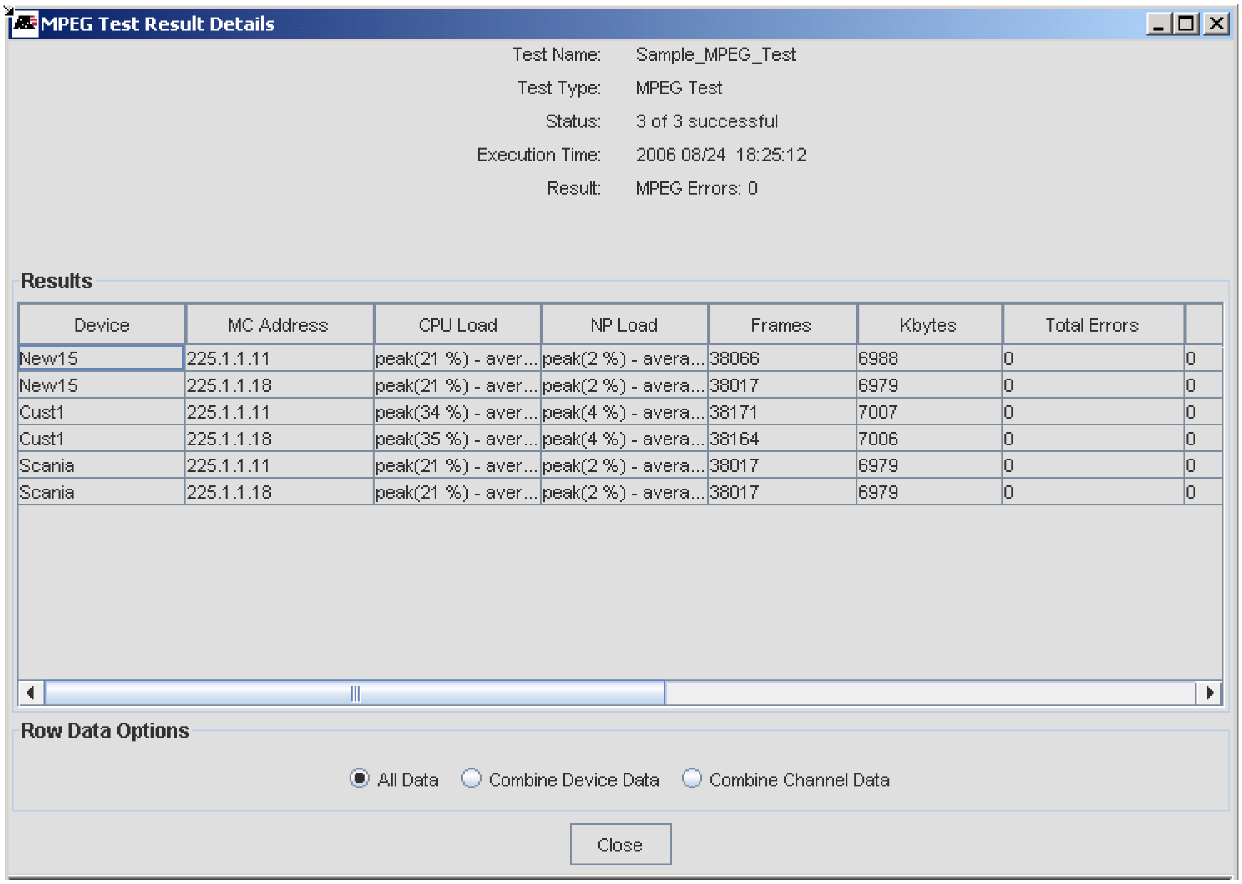


Total 1 Displaying 1 to 1 Page Length 25

Test Name	Type	Num Dev.	Status	Time	Results
Sample_MPEG_Test	MPEG Test	3	3 of 3 successful	2006 08/24 18:25...	MPEG Errors: 0

FIGURE 12-66 Viewing Test Results for MPEG Test

To review specific test results, double-click on a row in the table or right click on a row and select View Test Result MPEG Test Results Details panel, as shown in the following figure.



Test Name: Sample_MPEG_Test
Test Type: MPEG Test
Status: 3 of 3 successful
Execution Time: 2006 08/24 18:25:12
Result: MPEG Errors: 0

Results

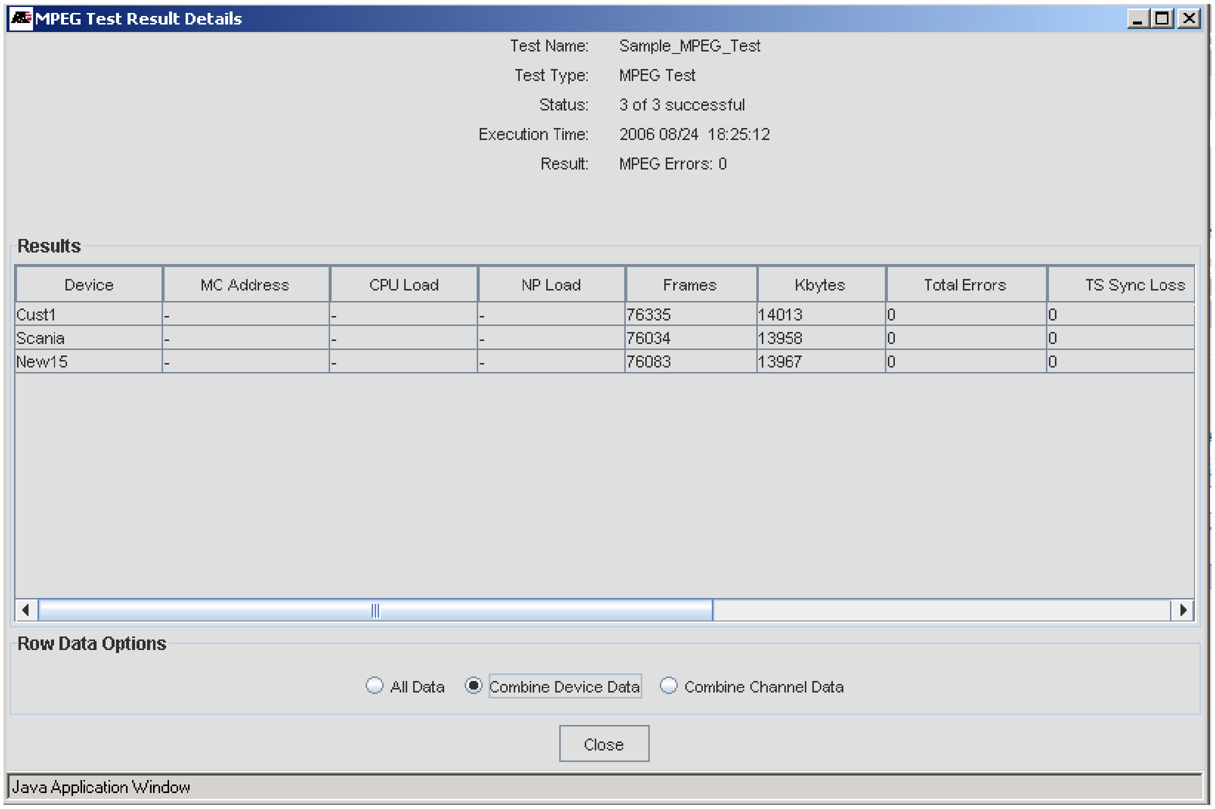
Device	MC Address	CPU Load	NP Load	Frames	Kbytes	Total Errors	
New15	225.1.1.11	peak(21 %) - aver...	peak(2 %) - avera...	38066	6988	0	0
New15	225.1.1.18	peak(21 %) - aver...	peak(2 %) - avera...	38017	6979	0	0
Cust1	225.1.1.11	peak(34 %) - aver...	peak(4 %) - avera...	38171	7007	0	0
Cust1	225.1.1.18	peak(35 %) - aver...	peak(4 %) - avera...	38164	7006	0	0
Scania	225.1.1.11	peak(21 %) - aver...	peak(2 %) - avera...	38017	6979	0	0
Scania	225.1.1.18	peak(21 %) - aver...	peak(2 %) - avera...	38017	6979	0	0

Row Data Options

● All Data ○ Combine Device Data ○ Combine Channel Data

FIGURE 12-67 Results of MPEG Network Test Execution - All Data

The “Combine Device Data” Radio button combines all the data from each iMG/RG into a single row entry, as shown below.



Test Name: Sample_MPEG_Test

Test Type: MPEG Test

Status: 3 of 3 successful

Execution Time: 2006.08/24 18:25:12

Result: MPEG Errors: 0

Results

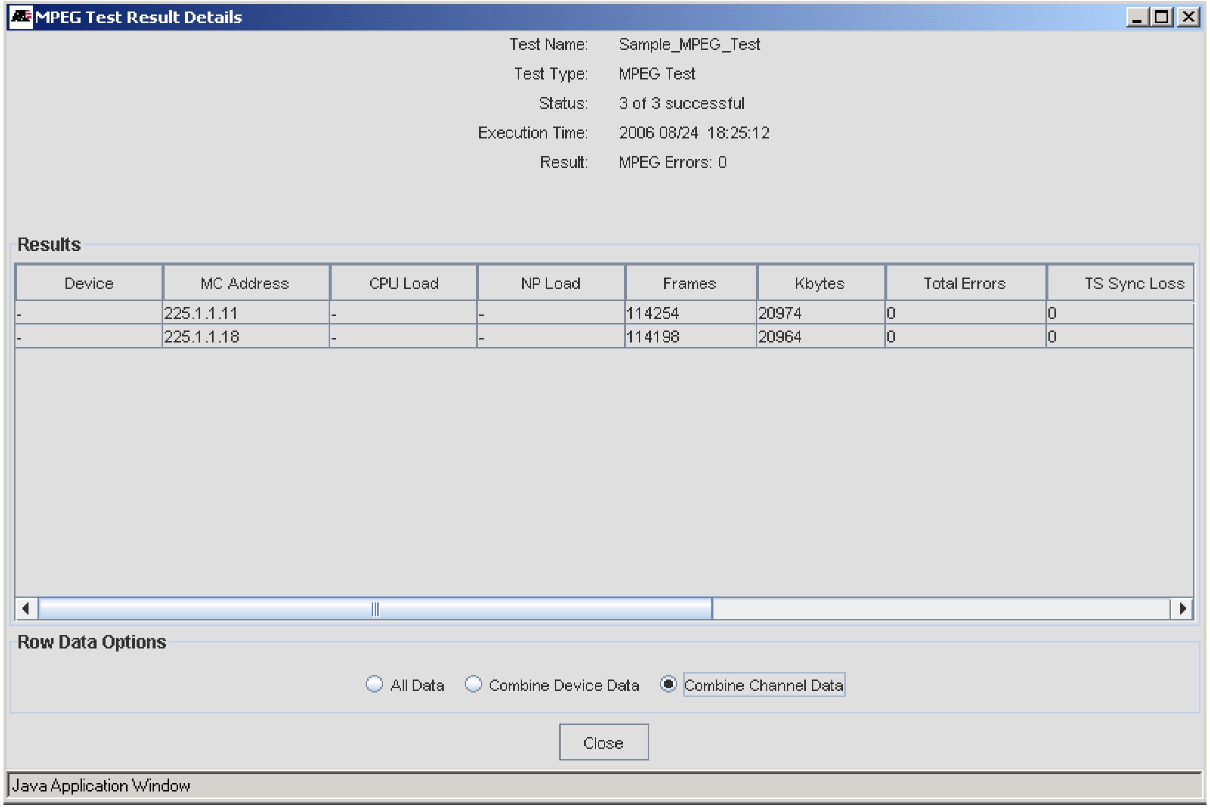
Device	MC Address	CPU Load	NP Load	Frames	Kbytes	Total Errors	TS Sync Loss
Cust1	-	-	-	76335	14013	0	0
Scania	-	-	-	76034	13958	0	0
New15	-	-	-	76083	13967	0	0

Row Data Options

○ All Data ● Combine Device Data ○ Combine Channel Data

FIGURE 12-68 Results of MPEG Network Test Execution - Combine Device Data

The “Combine Channel Data” Radio button combines all the data from each multicast into a single row entry, as shown below.



MPEG Test Result Details

Test Name: Sample_MPEG_Test
Test Type: MPEG Test
Status: 3 of 3 successful
Execution Time: 2006 08/24 18:25:12
Result: MPEG Errors: 0

Results

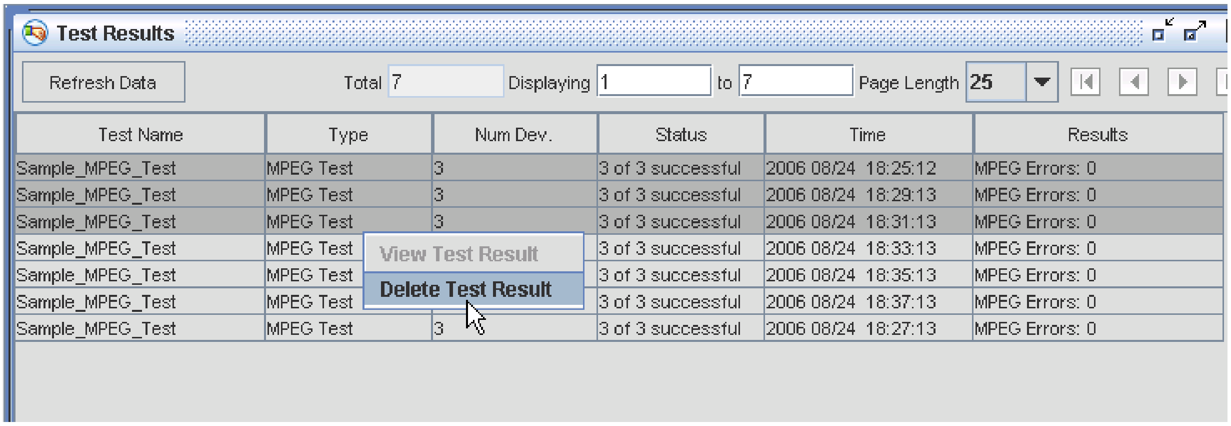
Device	MC Address	CPU Load	NP Load	Frames	Kbytes	Total Errors	TS Sync Loss
-	225.1.1.11	-	-	114254	20974	0	0
-	225.1.1.18	-	-	114198	20964	0	0

Row Data Options

○ All Data ○ Combine Device Data ● Combine Channel Data

FIGURE 12-69 Results of MPEG Network Test Execution - Combine Channel Data

To delete the test results, select one or more tests form the Test Results panel, right click, and select Delete Test Result. (Note that View Test Result is grayed out.) Refer to the following figure.



Total 7 Displaying 1 to 7 Page Length 25

Test Name	Type	Num Dev.	Status	Time	Results
Sample_MPEG_Test	MPEG Test	3	3 of 3 successful	2006 08/24 18:25:12	MPEG Errors: 0
Sample_MPEG_Test	MPEG Test	3	3 of 3 successful	2006 08/24 18:29:13	MPEG Errors: 0
Sample_MPEG_Test	MPEG Test	3	3 of 3 successful	2006 08/24 18:31:13	MPEG Errors: 0
Sample_MPEG_Test	MPEG Test		3 of 3 successful	2006 08/24 18:33:13	MPEG Errors: 0
Sample_MPEG_Test	MPEG Test		3 of 3 successful	2006 08/24 18:35:13	MPEG Errors: 0
Sample_MPEG_Test	MPEG Test		3 of 3 successful	2006 08/24 18:37:13	MPEG Errors: 0
Sample_MPEG_Test	MPEG Test	3	3 of 3 successful	2006 08/24 18:27:13	MPEG Errors: 0

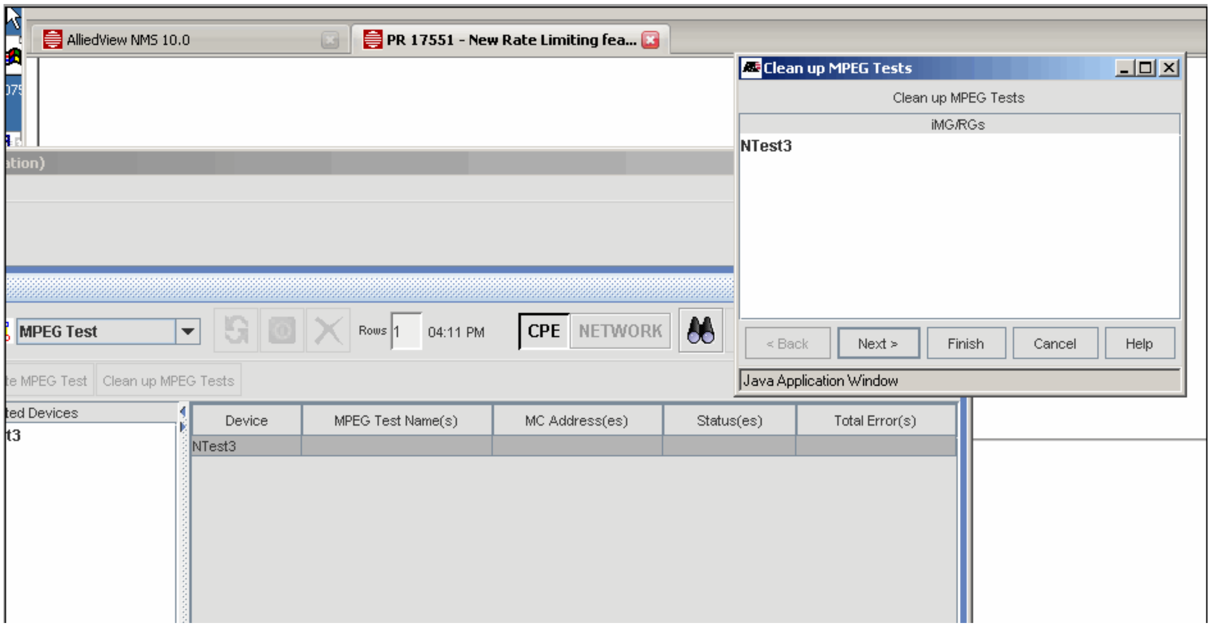
FIGURE 12-70 Deleting MPEG Test Results

To modify the schedule/recurrence of a test, select *Tools -> View Tasks,* and select the Task Name (the Name entered for the test) form the View Tasks table. Select **View Details**, and then the **Modify Schedule** button. Note that only the time of the test, not the other attributes, can be changed.

The steps to delete an MPEG test is similar to modifying its schedule. Select the Task Name (in this case Sample_MPEG_Test) and Click on **Remove**. This does not remove the results that the test produced; however, every day test results older than seven days are removed from the database.

To clean up the MPEG tests that have been run on multiple iMGs/RGS, the button **Clean up MPEG Tests** has been added in release 10.0 SP2. The user selects the iMGs/RGs, and the button is activated. When selected, the Clean up MPEG Tests panel appears, with the iMGs/RGs listed. The user can then select Finish to perform the clean up immediately, or Next to bring up a schedule. Refer to the following figure.

Note: These tests are usually ones that have failed for some reason, or been saved.



NTest3

Rows 1 04:11 PM

Device	MPEG Test Name(s)	MC Address(es)	Status(es)	Total Error(s)
NTest3				

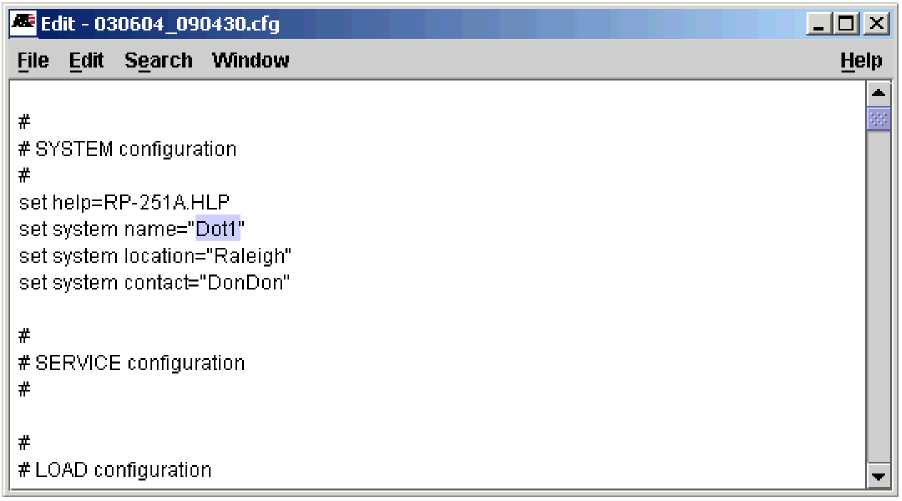
FIGURE 12-71 MPEG Test Clean Up Panel

12.2.15 Using the Edit Functions

The Edit window has the same functions for both the Command Script Management and Configuration File Management functions, and so the explanation for how the window works can apply to both types of files.

In the Command Script application, the **Edit** window brings up the unloaded multi-paged editor. The editor has Open and Save as buttons that work with the server file system. Selecting *File -> Open* in the **Edit** window brings up the NMS file system in the **Open** window. From the **Open** window, a file can be chosen. The *File -> Save* option uses whichever file was opened. The editor also has find, find next, and cut/copy/paste options.

When a file is open, the file text appears. In the following example a script file is opened. Refer to Figure 12-72.



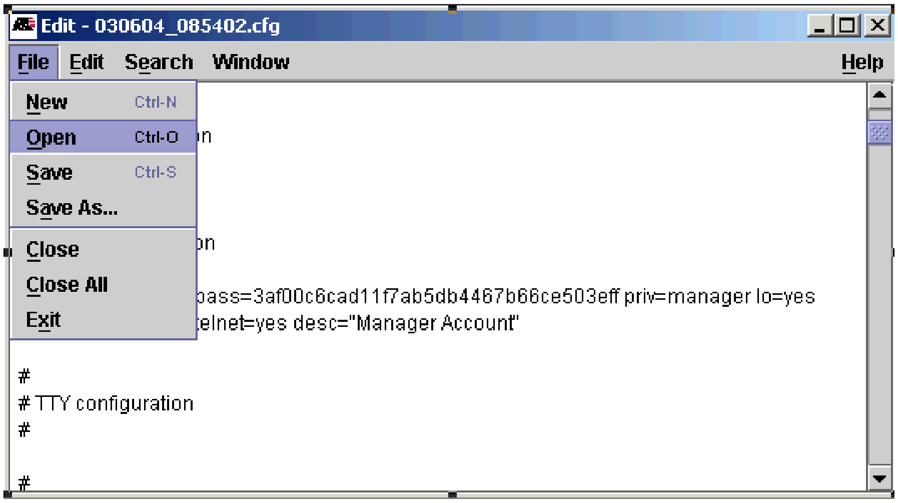
```
#
# SYSTEM configuration
#
set help=RP-251A.HLP
set system name="Dot1"
set system location="Raleigh"
set system contact="DonDon"

#
# SERVICE configuration
#

#
# LOAD configuration
```

FIGURE 12-72 Edit Window for Script Mgt Files

In the Configuration File Management application, the Edit button will display, if it is shown in the Default File column, the default configuration file. Otherwise it will display an open Edit window, the same as the Command Script application.

12.2.15.1 File Menu

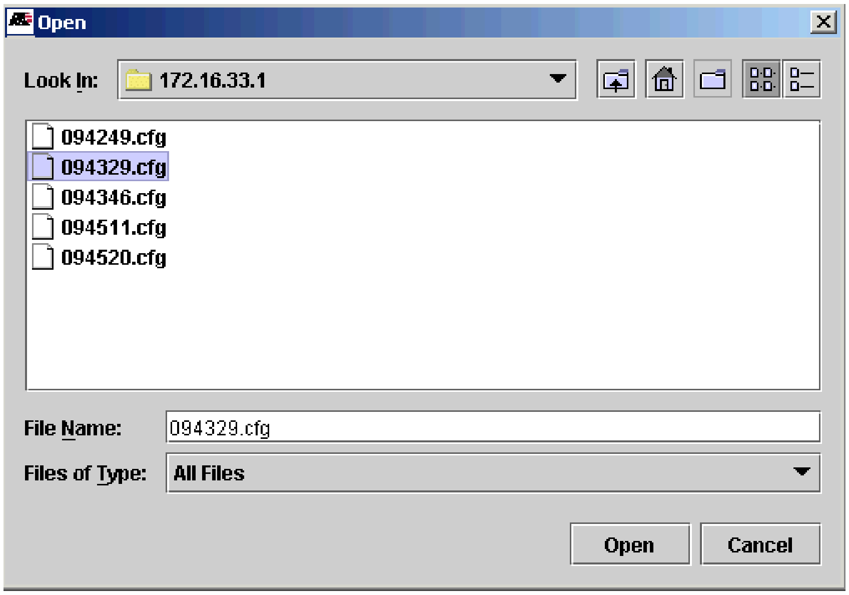
The *File* menu contains conventional options. *Open* and *Save As* can access the client's file system or the server's file system depending on a toggle on the file chooser dialog. *Save* will save the current file to whichever file system from which it was opened. *Close* and *Close All* are required since this is a multi-page editor. Refer to Figure 12-73 for the **Edit** window and the *File* pull-down menu. The example is for a command script file.



```
n


on

pass=3af00c6cad11f7ab5db4467b66ce503eff priv=manager lo=yes
elnet=yes desc="Manager Account"

#
# TTY configuration
#

#
```

FIGURE 12-73 File Pull-down for Edit of Scripts

Selecting the *File -> Open* menu item brings up a listing of the latest files from the server file system for the devices highlighted on the **Command Script Mgmt** panel when the editor was launched. Files can be viewed as a simple list or with details (Size, Type, when Modified). Template files can also be created and included. Refer to Figure 12-74 and Figure 12-75.



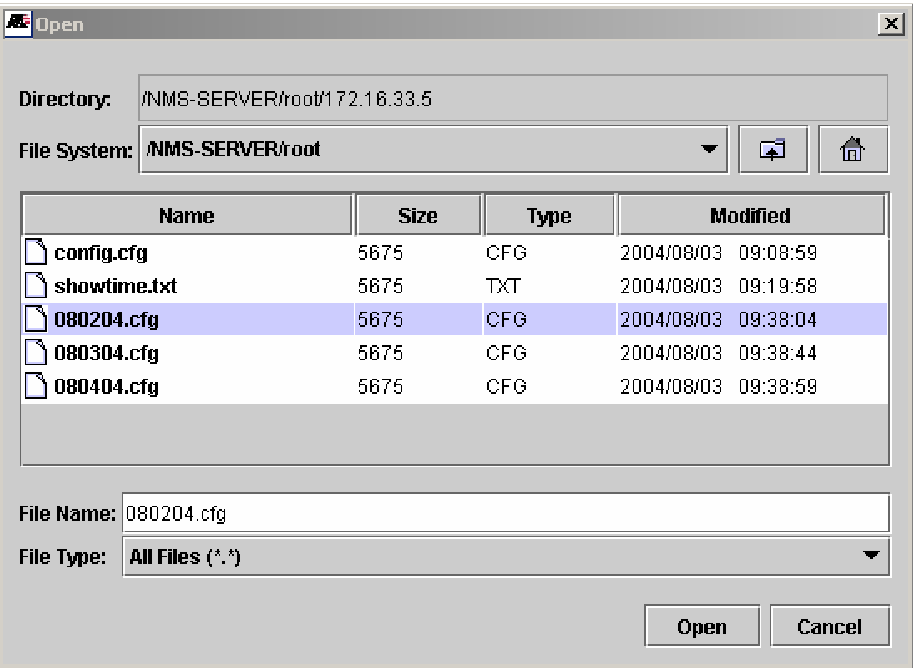
Look In: 172.16.33.1

094249.cfg
094329.cfg
094346.cfg
094511.cfg
094520.cfg

File Name: 094329.cfg

Files of Type: All Files

FIGURE 12-74 Files Available for Edit from Server File System (List View)



Directory: /NMS-SERVER/root/172.16.33.5

File System: /NMS-SERVER/root

Name	Size	Type	Modified
config.cfg	5675	CFG	2004/08/03 09:08:59
showtime.txt	5675	TXT	2004/08/03 09:19:58
080204.cfg	5675	CFG	2004/08/03 09:38:04
080304.cfg	5675	CFG	2004/08/03 09:38:44
080404.cfg	5675	CFG	2004/08/03 09:38:59

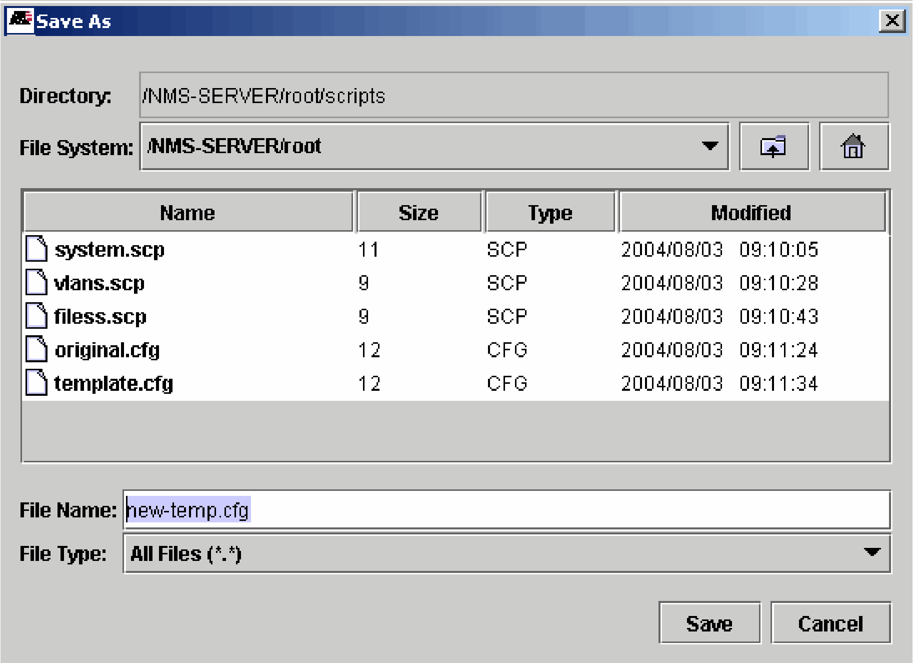
File Name: 080204.cfg

File Type: All Files (*.*)

FIGURE 12-75 Files Available for Edit from Server File System (Details View)

Once a file is opened and edited, it can be saved on the Server File System. Files can be saved as templates for future script writing. Refer to Figure 12-76.

Note: Since files are being saved to the server (rather than a device), unrestricted filenames and extensions are allowed.



Directory: /NMS-SERVER/root/scripts

File System: /NMS-SERVER/root

Name	Size	Type	Modified
system.scp	11	SCP	2004/08/03 09:10:05
vlans.scp	9	SCP	2004/08/03 09:10:28
filess.scp	9	SCP	2004/08/03 09:10:43
original.cfg	12	CFG	2004/08/03 09:11:24
template.cfg	12	CFG	2004/08/03 09:11:34

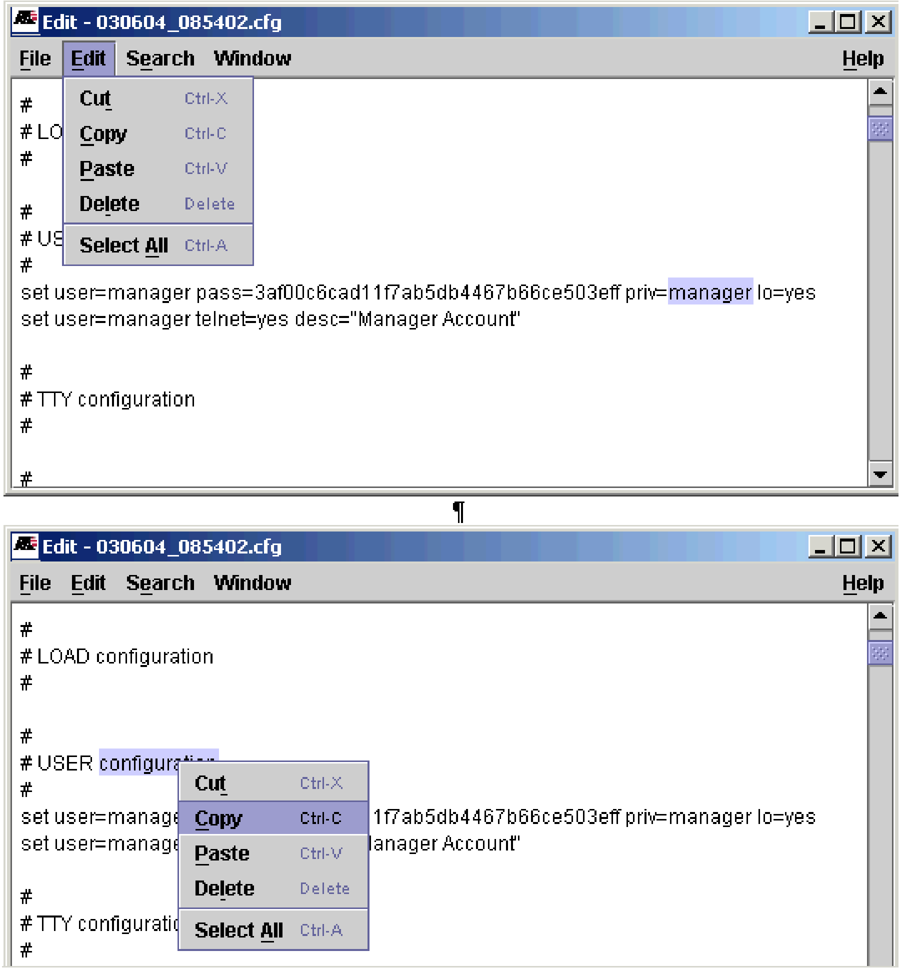
File Name: new-temp.cfg

File Type: All Files (*.*)

FIGURE 12-76 Saving Files after Editing

12.2.15.2 Edit Menu

The *Edit* menu has conventional options (CUt, Copy, Paste, Delete, Select All). Right-clicking in the text area will bring up these options as well. Refer to Figure 12-77.



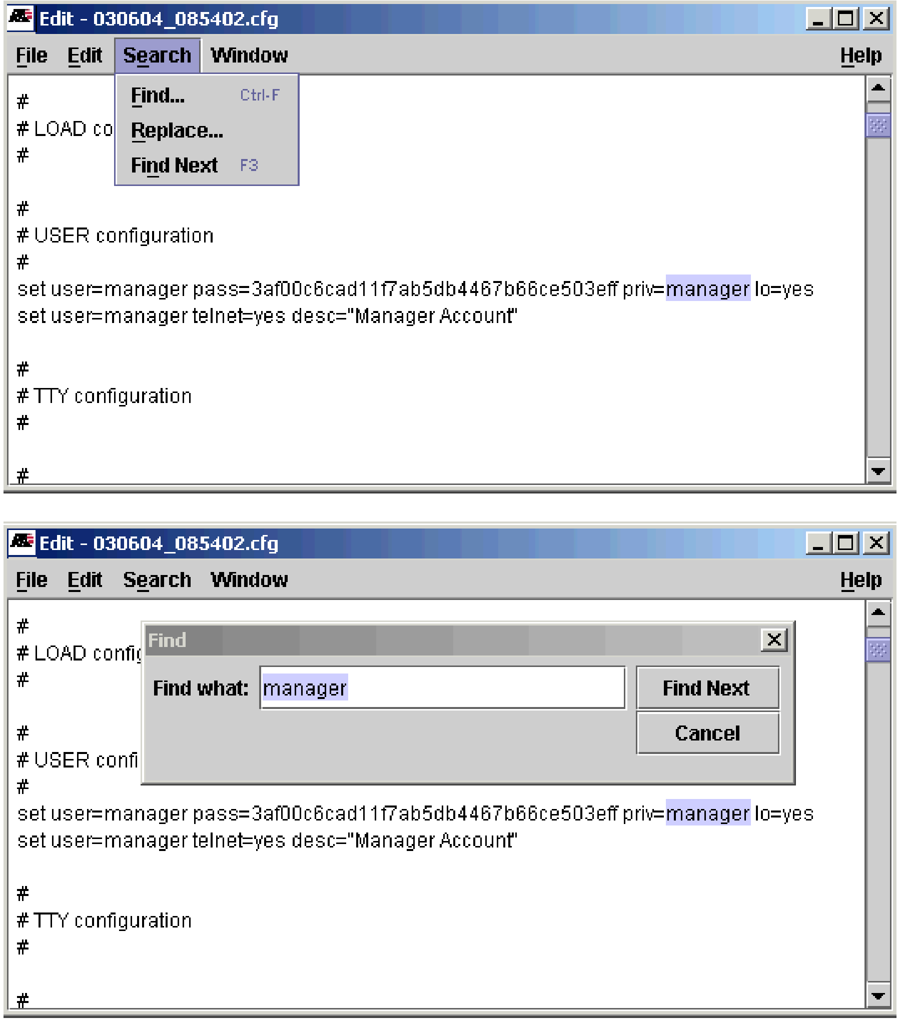
```
#
# LO
#

#
# US
#
set user=manager pass=3af00c6cad11f7ab5db4467b66ce503eff priv=manager lo=yes
set user=manager telnet=yes desc="Manager Account"

#
# TTY configuration
#

#
```

```
#
# LOAD configuration
#

#
# USER configura
#
set user=manage                 1f7ab5db4467b66ce503eff priv=manager lo=yes
set user=manage                lanager Account"

#
# TTY configuratic
#
```

FIGURE 12-77 Edit Menu Options for Text Files

12.2.15.3 Search Menu

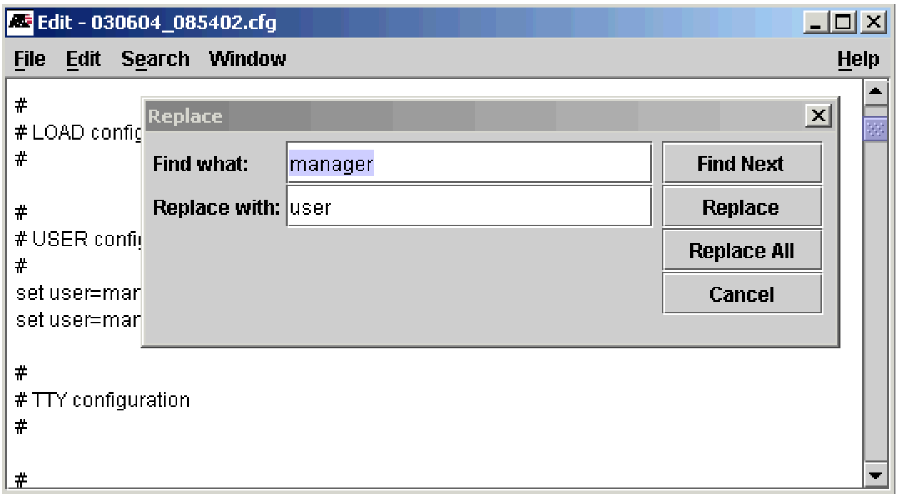
The *Search* menu provides for searching within the current window. Conventional *Find* and *Replace* options are provided. Refer to the following figures.



```
#
# LOAD co
#

#
# USER configuration
#
set user=manager pass=3af00c6cad11f7ab5db4467b66ce503eff priv=manager lo=yes
set user=manager telnet=yes desc="Manager Account"

#
# TTY configuration
#

#
```

Find what: manager

FIGURE 12-78 Search Find Option



Find what: manager

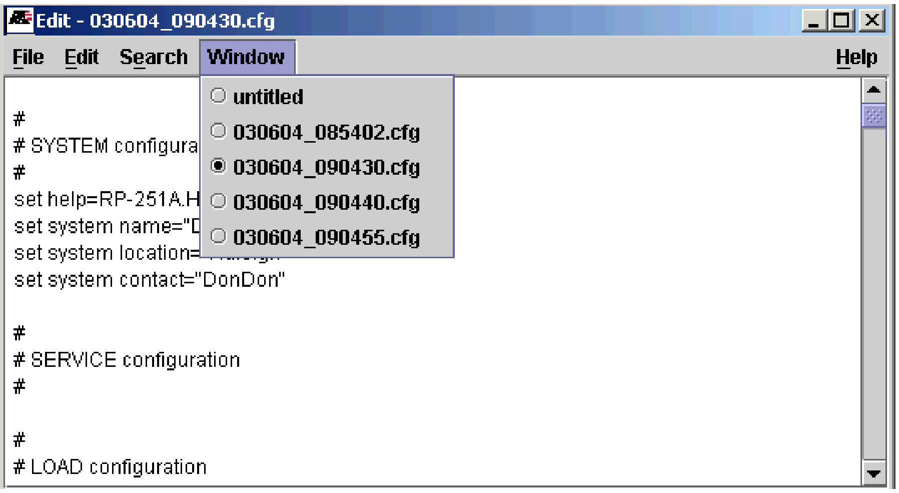
Replace with: user

```
#
# LOAD config
#

#
# USER confi
#
set user=mar
set user=mar

#
# TTY configuration
#

#
```

FIGURE 12-79 Search Replace Option

12.2.15.4 Window Menu

The Window menu provides changing between open files. Each time a file is entered, the cursor, text selections, and scroll bar are in the same state they were in when that file was left. The Window menus changes dynamically as files are opened, created, and closed.



```
#
# SYSTEM configura
#
set help=RP-251A.H
set system name="D
set system location=
set system contact="DonDon"

#
# SERVICE configuration
#

#
# LOAD configuration
```

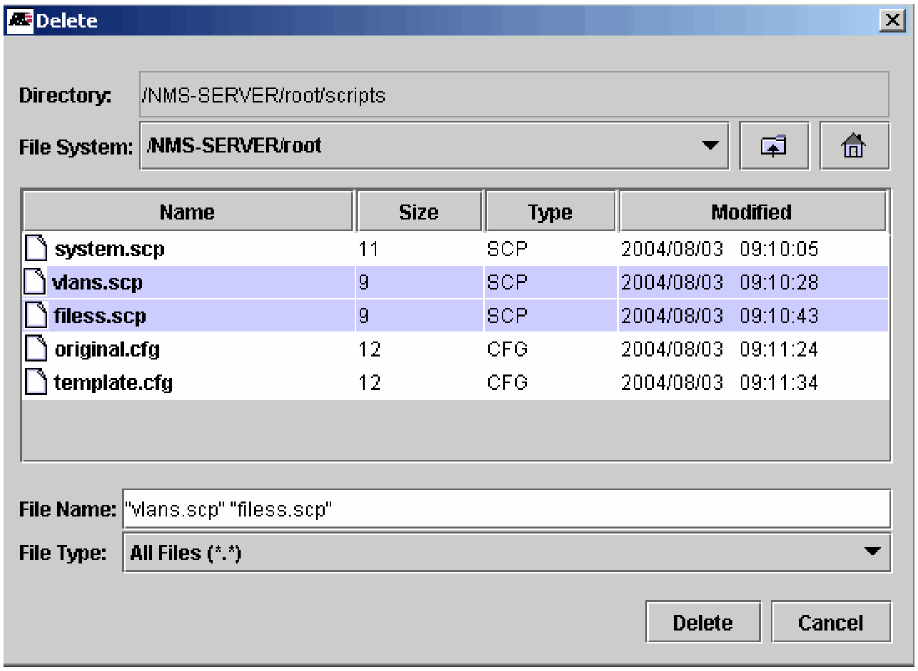
FIGURE 12-80 Window Menu for File Editor

12.2.16 Using the Delete Function

The **Delete Files** Button invokes the same window for both Command Script Management and Configuration File Management, and so the explanation for how the window works can apply to both types of files.

With no devices selected, the Delete button brings up a file chooser that provides navigation among all the user's directories and lets the user delete one or more files from the same directory. Select one or more files to delete:

When the files for deletion for a device are listed, the user can select the details icon and see the file properties, as shown in the following figure.



Directory: /NMS-SERVER/root/scripts

File System: /NMS-SERVER/root

Name	Size	Type	Modified
system.scp	11	SCP	2004/08/03 09:10:05
vlans.scp	9	SCP	2004/08/03 09:10:28
filess.scp	9	SCP	2004/08/03 09:10:43
original.cfg	12	CFG	2004/08/03 09:11:24
template.cfg	12	CFG	2004/08/03 09:11:34

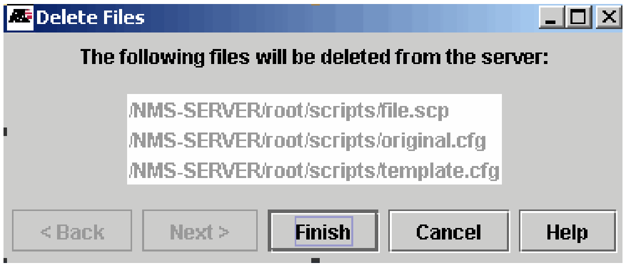
File Name: "vlans.scp" "filess.scp"

File Type: All Files (*.*)

FIGURE 12-81 Delete File Window for Multiple File and Properties

The current directory is displayed at the top. Just below is a pull-down combo box that can be used to jump between file system roots-in this case /NMS-SERVER/root/scripts and /NMS-SERVER/root. The folder and home icons can be used to navigate up in a directory tree or to jump to the “home” directory, which is usually the user's home directory. File properties (size, type, and date last modified) are always displayed. File types can be filtered with the pull-down combo box at the bottom.

The Delete button will prompt to confirm the files to delete, as shown in the following figure.

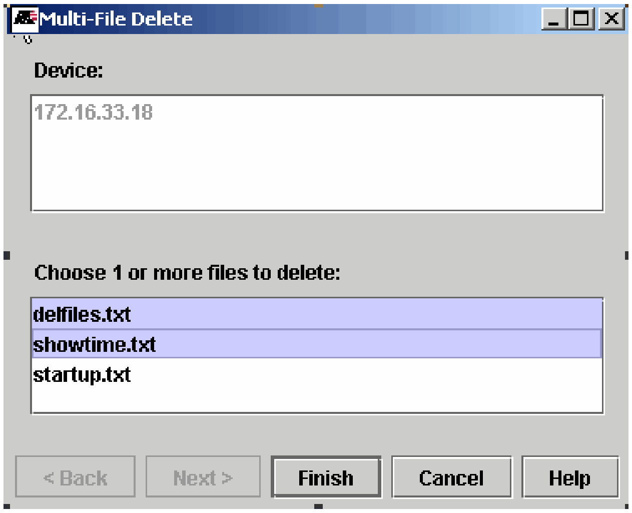


The following files will be deleted from the server:

/NMS-SERVER/root/scripts/file.scp
/NMS-SERVER/root/scripts/original.cfg
/NMS-SERVER/root/scripts/template.cfg

FIGURE 12-82 Confirm Files to Delete

With one or more devices selected, a Multi-File Delete wizard pops up instead of the file chooser. For a single device, this wizard lists all the files in the user's device directory and provides no way to navigate to other directories. It provides a quicker way to delete one or more files for a single device. Refer to the following figure.



Multi-File Delete

Device:

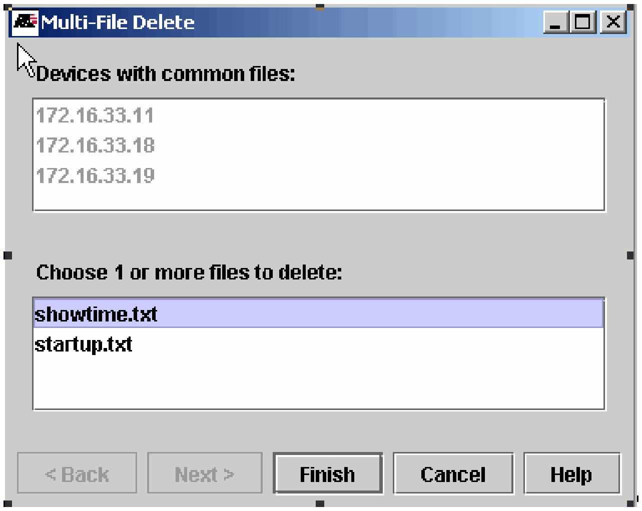
172.16.33.18

Choose 1 or more files to delete:

delfiles.txt
showtime.txt
startup.txt

FIGURE 12-83 Multi-File Delete Window

With two or more devices selected, this wizard displays all the files with names *common to all the selected devices*. Files with any other names will be left out. No file properties or pathnames can be displayed since they may differ among the various devices even though the file names are the same. This wizard will delete selected files from all the device directories in one operation. Refer to the following figure.



Multi-File Delete

Devices with common files:

172.16.33.11
172.16.33.18
172.16.33.19

Choose 1 or more files to delete:

showtime.txt
startup.txt

FIGURE 12-84 Multifile Delete Window - Files Common to All Devices

If there are no common files among the selected devices, and error message pops up, **There are no common files for the selected devices.**

Note: Files in the user's scripts directory are not associated directly to a device and can therefore only be deleted with the file chooser version of this dialog (brought up with no devices selected).

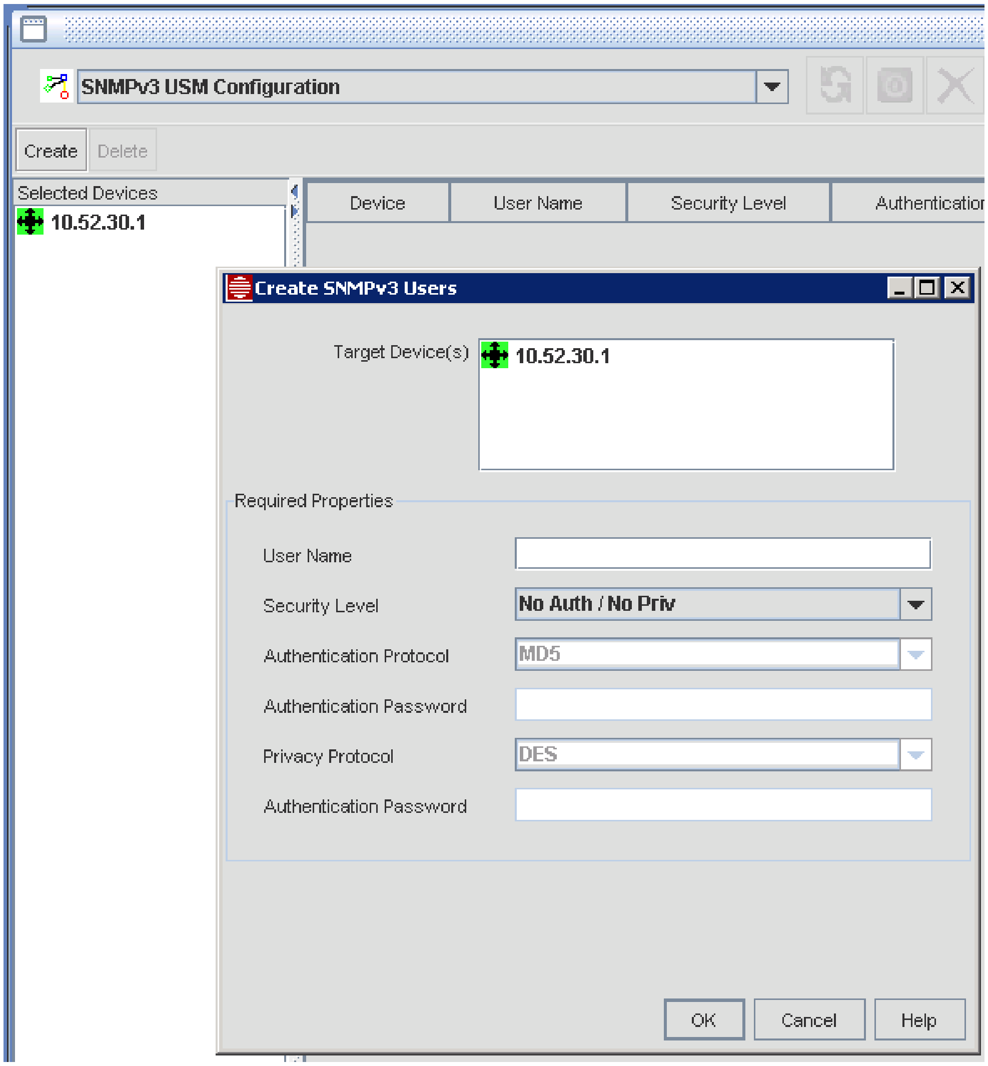
12.2.17 SNMPv3 USM Configuration

This SNMPv3 uses the User-Based Security Model (USM) and is specified in RFC2574. The USM has the concept of multiple users where each user provides secret keys for authentication and privacy. The authentication protocols specified for use are HMAC-MD5 and HMAC-SHA. The privacy protocol specified is CBC-DES.

From the panel the administrator can activate this model for one or devices, similar to other MDTI applications.

The fields filled in when the administrator creates an SNMPv3 user.

Refer to the following figure.



Target Device(s) 10.52.30.1

Required Properties

User Name

Security Level No Auth / No Priv

Authentication Protocol MD5

Authentication Password

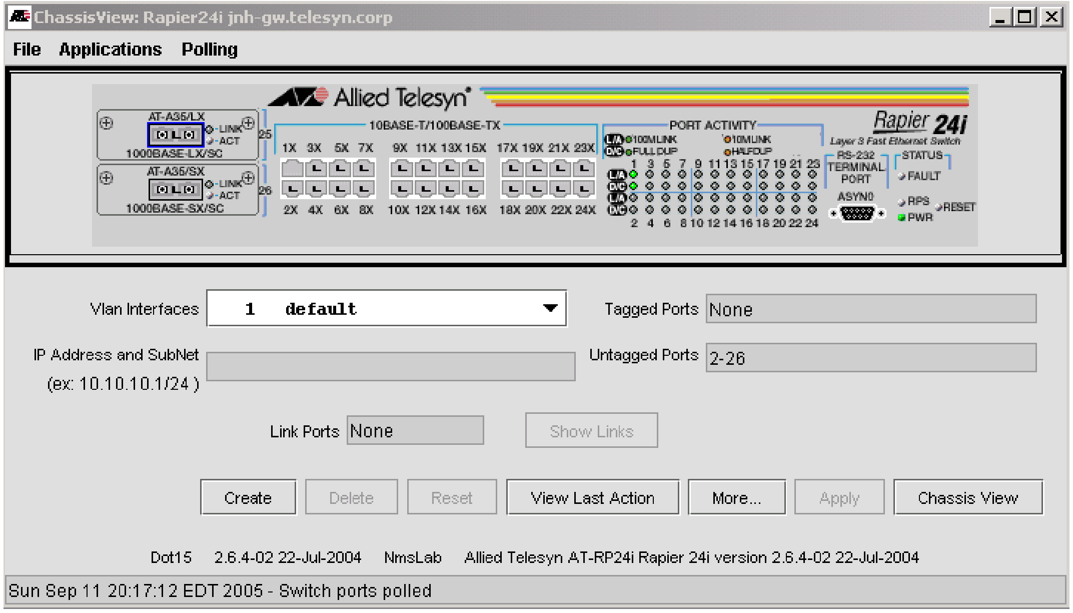
Privacy Protocol DES

Authentication Password

FIGURE 12-85 SNMPv3 USM Configuration Panel

12.3 Configure VLAN (Chassis View)

To configure a VLAN for a single device, right-click the device, and then select **Provision** > **Configure VLAN**. The VLAN chassis configuration screen opens and fills in the present VLAN configuration. The Chassis view and VLAN Configuration view are combined, but the VLAN-related information will change depending on the VLAN interface chosen. Refer to the following figures for examples of the configuration screen.



Vlan Interfaces 1 default

Tagged Ports None

IP Address and SubNet (ex: 10.10.10.1/24)

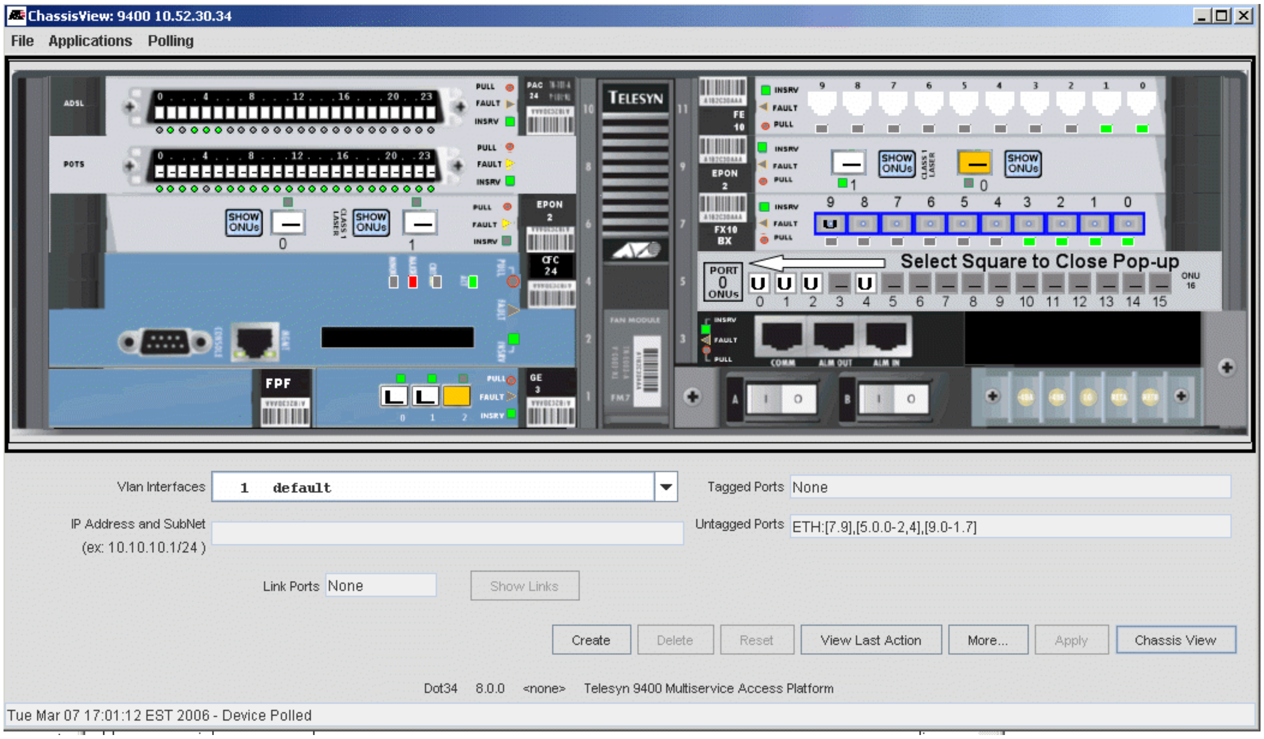
Untagged Ports 2-26

Link Ports None

Dot15 2.6.4-02 22-Jul-2004 NmsLab Allied Telesyn AT-RP24i Rapier 24i version 2.6.4-02 22-Jul-2004

Sun Sep 11 20:17:12 EDT 2005 - Switch ports polled

FIGURE 12-86 VLAN Configuration Screen (Rapier Device)



Vlan Interfaces 1 default

Tagged Ports None

IP Address and SubNet (ex: 10.10.10.1/24)

Untagged Ports ETH:[7.9],[5.0.0-2,4],[9.0-1.7]

Link Ports None

Dot34 8.0.0 <none> Telesyn 9400 Multiservice Access Platform

Tue Mar 07 17:01:12 EST 2006 - Device Polled

FIGURE 12-87 VLAN Configuration Screen (iMAP Device)

The following table gives an overview of the fields, graphics, and buttons available.

TABLE 12-10 VLAN Configuration Options

Screen Item	Description
Create	If creating a VLAN on the device, select this button first. You will see a **Create New VLAN** form. Fill in the Name and ID, and then click **OK**, and the VLAN is added to the Vlan Interfaces pull-down.
Vlan Interfaces	The VLAN interfaces available on the device. This includes all VLAN interfaces.
IP Address and Subnet	If this Vlan interface is part of an IP-based Network VLAN, this is included. The format is the IP address and the subnet mask. The subnet can be specified by a forward slash and the mask as a number of bits (e.g. /24) or by a space and the full dot notation (e.g. 255.255.255.0).
Untagged Ports	For the selected VLAN interface, the ports that are reserved. On the graphic, these have the capital letter **U**.
Tagged Ports	For the selected VLAN, the ports that are reserved and active. On the graphic, these have the capital letter **T**.
Translated Port	For the selected VLAN, allows the user to specify the VLAN on the customer side of the port that will be translated into the selected VLAN. When selecting X, the user will see a pop-up window that allows the user to input the translate from ID. Once entered, these have the graphic capital letter **X**.
VC-0 through VC-3 buttons	When more than one VC has been associated with a VLAN, each button, when selected, show the VLANs which have that VC provisioned. (This is for iMAP devices only.)
Link Ports	These are the ports that are used for connection to another device and are used as part of one or more Network VLANs including the current VLAN. On the display, these will be identified with the capital letter **L**. A Link Port cannot be changed from the VLAN Configuration screen. It must be changed on both ends of the link using the Create Vlan, Extend Vlan, or Delete Link applications. However, a Link Port can be changed in the VLAN Interface Configuration application, which is a similar application that is launched on VLAN interfaces either from a VLAN Map or a VLAN Interface row in one of the Inventory tables. In this application, Link Ports can be toggled from **L** (not part of the VLAN) to **lu** (linked untagged), to **lt** (linked tagged). This is useful for repairing VLAN entries that have become inconsistent with the entry for the device at the other end of the link
Rapier Specific Vlan Parameters	These apply only to VLANs on Rapier-type devices, and are divided into two areas: 1. **Device Wide Parameters** - These are read -only and display device-level attributes as Enabled or Disabled: - IGMP Status - IP Multicast Hardware Switching - OSPF Status - PIM Status 2. **VLAN Interface Parameters** - These are read-write and apply only to the selected VLAN: - IGMP Enabled - OSPF Area - Set the Open Shortest Path First Area - OSPF Metric - Set the Open Shortest Path First Metric - PIM Mode

TABLE 12-10 VLAN Configuration Options

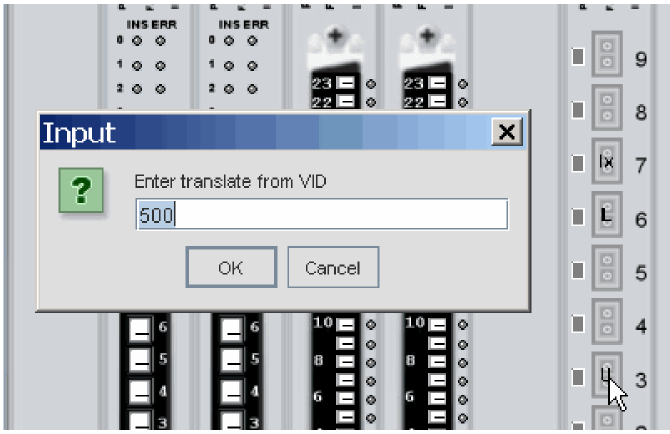
Screen Item	Description
iMAP Specific Parameters	These apply only to iMAP devices, and are divided into two areas: 1. **Device Wide Parameters** - These are read -only and display device-level attributes as Enabled or Disabled: - Access Interface - This is the IP interface the device is using to communicate with the NMS. Options are MGMT (for the Ethernet interface that transports only management data packets) or the IP address of inband interface (in-band Ethernet interface that interleaves user data packets with management data packets on the uplink, using a VLAN interface). - IGMP - Whether IGMP has been Enabled or Disabled for the device. This attribute is displayed as a device-wide parameter for devices running iMAP software up through release 16.x.x. 2. **VLAN Interface Parameters** - These are read-only and apply only to the selected VLAN: - Double Tagged (HVlan) - If the selected VLAN is an HVLAN (and will therefore be a VLAN used to switch the traffic across the network), this is shown as TRUE. Refer to Section 6. - Translation Ports - When the VLAN chosen is a translation VLAN (where a service provider takes a customer VID and translates it into a unique VLAN ID for transport across the network), this field contains the ports the translation VLAN ID resides on. Refer to Section 6. Note that HVlan and Translation are mutually exclusive features. - Forwarding Mode - Displays the current state of VLAN forwarding. You can change it to Standard or Upstream for the selected VLAN. - IGMP Snooping - Displays the current state of IGMP Snooping. You can enable or disable IGMP Snooping for the selected VLAN.
Create	Create a new VLAN. A Create New VLAN form will appear, with the default name and number one that has not been used yet.
Delete	Allows the user to delete the selected VLAN. (Note that since the default VLAN [VID 1] cannot be deleted, this button is inactive when the selected VLAN is VLAN 1.)
Reset	Cancels the changes that were made using the graphic. The graphic reverts to the original port assignments.
Apply	Makes and confirms the port assignment changes. If any errors occur, (such as a conflict with another user making port changes), there is an error message and the history window is displayed.
Less/More	This shows/hides the additional attributes, one for Rapier-specific Vlan parameters, one for iMAP-specific VLAN parameters, such as specific translations. These are explained above.
Show Links	If the VLAN is configured as part of a Network VLAN, selecting this button will show the physical links over which the logical VLAN links are configured.
View Last Action	This will open up the Recent Commands... window and show what command and response were involved in the last action on the form.
Close	Closes the form. If this VLAN Configuration form is invoked from the Chassis View, the Close button is replaced with the Chassis View button, to return to the first view of the device.

Note: To see the status of a port, place the cursor over a port in the graphic and a tooltip appears, which shows the permitted states for that port. Allowed states are Plain, Tagged, Untagged, Linked-Tagged, Unlink-Tagged, Linked, and Translated. (The actual states available depend on the configuration.) If a port is Plain, the user can then click on the port and cycle the status from U (untagged) to T (tagged) to X (translated). Clicking on the port again will return the port to blank. When a port is marked as untagged for a VLAN other than the default VLAN, that port can only be marked as tagged for the other VLANs. In this case the port alternates only between tagged and blank.

Note: For the EPON2 card, the user can click on the ONUs button and a pop-up will show the VLAN status of the ONU ports. To close the pop-up, click on the square labeled Port <no.> ONUs, as highlighted in Figure 12-87.

Note: To change the status for a set of ports, select and hold the SHIFT key and then click and drag the left mouse button over multiple ports.

Caution: The FE/FX10 cards have certain restrictions on VLAN translations, and the user must be aware of these so as not to compromise service. Refer to "Restrictions" on page 566.


Input

Enter translate from VID

500

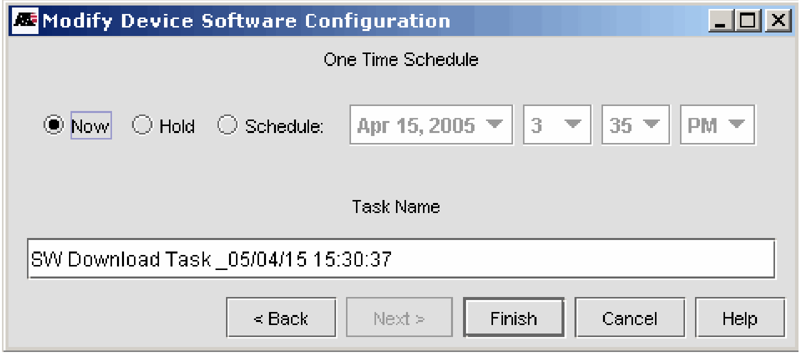
FIGURE 12-88 Entering a translated VLAN (State will go from U to X)

12.4 Managing Tasks

You can schedule and control how provisioning tasks are executed in the NMS. You can schedule tasks to occur one time or on a recurring basis.

12.4.1 Scheduling One Time Tasks

When a task happens only once, the **One Time Schedule** form allows you to schedule when the task will occur.


Modify Device Software Configuration

One Time Schedule

● Now ○ Hold ○ Schedule: Apr 15, 2005 3 35 PM

Task Name

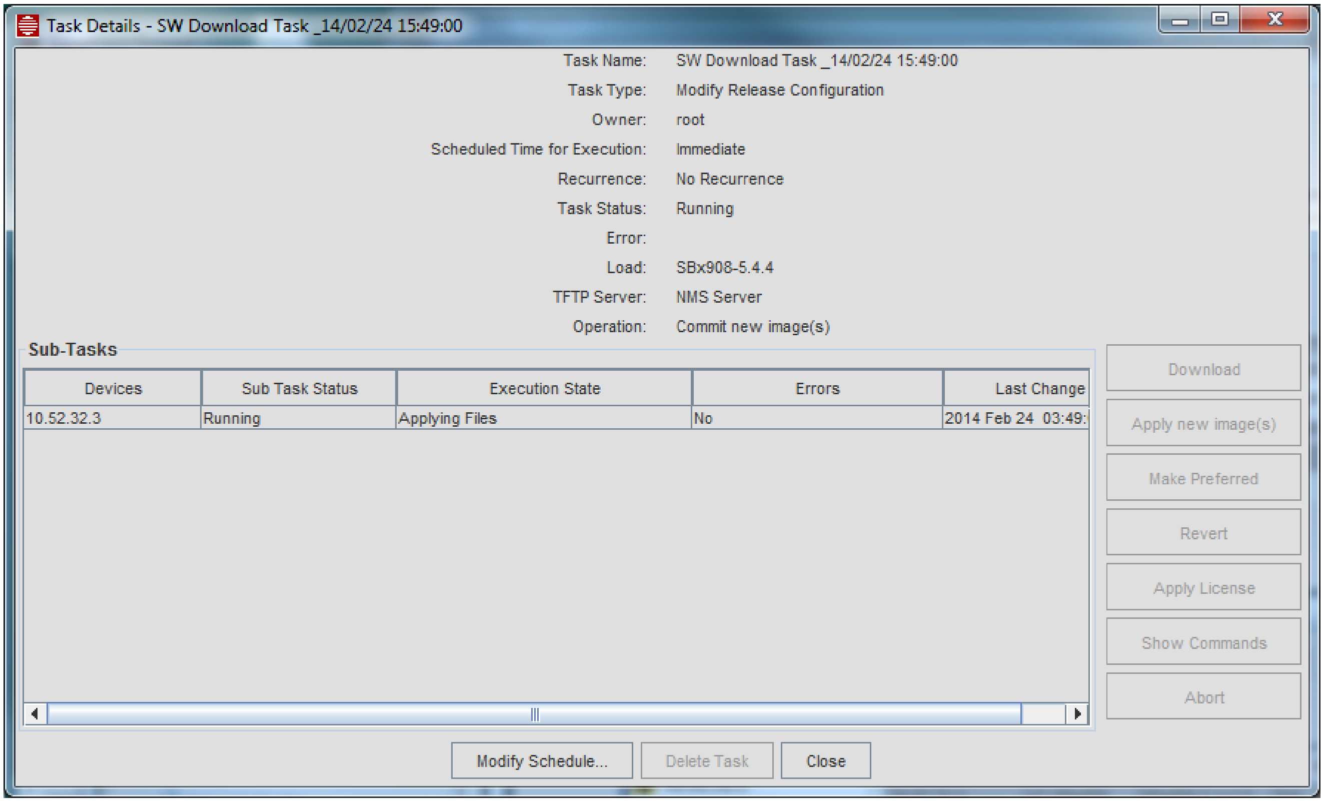
SW Download Task _05/04/15 15:30:37

FIGURE 12-89 One-time Task Form

Select one of the following:

- **Now** - Begin the task as soon as the NMS is able to perform it.
- **Hold** - Place the task in the Task List table to perform it at another time. You must modify the task when you are ready for the NMS to perform it. Tasks are held in the Task List table until you modify them.
- **Schedule** - Perform the task at a specific date and time. Select the date and time from the drop-down lists.

If you select **Now**, the **Task Details** form appears. **Task Details** provides the attributes, status, and options for the task.



Task Name: SW Download Task _14/02/24 15:49:00
Task Type: Modify Release Configuration
Owner: root
Scheduled Time for Execution: Immediate
Recurrence: No Recurrence
Task Status: Running
Error:
Load: SBx908-5.4.4
TFTP Server: NMS Server
Operation: Commit new image(s)

Sub-Tasks

Devices	Sub Task Status	Execution State	Errors	Last Change
10.52.32.3	Running	Applying Files	No	2014 Feb 24 03:49:

FIGURE 12-90 Task Details Form

Double-click on a task to see the details and status of the task.

The following options apply to software download tasks:

- **Download** - Download the software load and any required license files onto the device. The software load and license files must be in the **<NMS_Home>/swdownload** directory.
- **Apply new image(s)** - Apply the load files to the device so that the device is running with the new load.
- **Make Preferred** - Make the load file the preferred load for the device.
- **Revert** - Bring the device back to the state it was in before the new software load was downloaded to the device.
- **Apply License** - Activate the software license on the device. If it is an iMAP device, you must download the software load and license files to the device before applying the license. If it is an AlliedWare Plus device, you do not need to download the license separately before applying it.

The following options apply to all tasks:

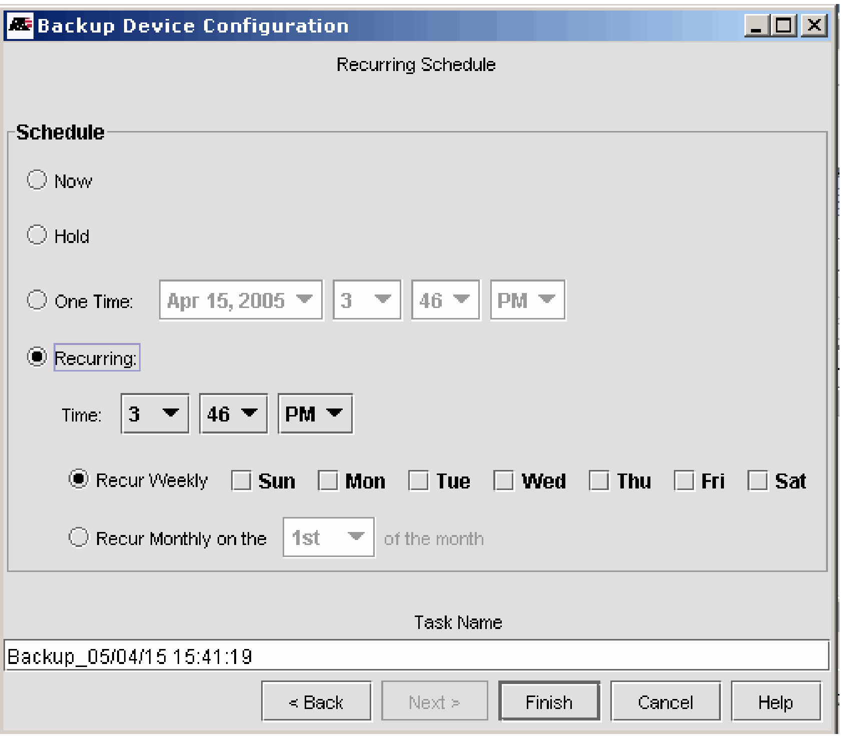
- **Show Commands** - Display the CLI commands the task is executing and any error messages that result from performing the task.
- **Abort** - Stop the running task.

If the task is not currently running, the following options are available:

- **Modify Schedule** - Change when the NMS will perform the task.
- **Delete Task** - Remove the task from the list.

12.4.2 Recurring Tasks

The **Recurring Schedule** form allows you to schedule the time and frequency of a recurring task.



Backup Device Configuration

Recurring Schedule

Schedule

○ Now

○ Hold

○ One Time: Apr 15, 2005 3 46 PM

● Recurring:

Time: 3 46 PM

● Recur Weekly □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

○ Recur Monthly on the 1st of the month

Task Name

Backup_05/04/15 15:41:19

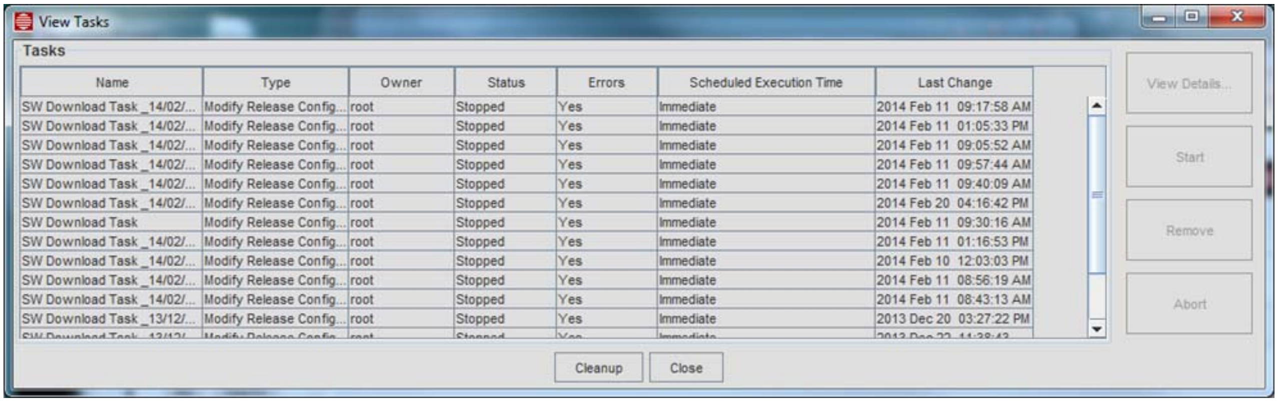
FIGURE 12-91 Recurring Task Form

You can schedule recurring tasks to occur on a weekly or montly basis. Recurring tasks appear in the Task List table.

12.4.3 Viewing Tasks

All tasks appear in the Task List table.

To open the Task List table, from the main menu, select **Tools > View Tasks**. The **View Tasks** window appears.



View Tasks

Tasks

Name	Type	Owner	Status	Errors	Scheduled Execution Time	Last Change
SW Download Task _14/02/...	Modify Release Config...	root	Stopped	Yes	Immediate	2014 Feb 11 09:17:58 AM
SW Download Task _14/02/...	Modify Release Config...	root	Stopped	Yes	Immediate	2014 Feb 11 01:05:33 PM
SW Download Task _14/02/...	Modify Release Config...	root	Stopped	Yes	Immediate	2014 Feb 11 09:05:52 AM
SW Download Task _14/02/...	Modify Release Config...	root	Stopped	Yes	Immediate	2014 Feb 11 09:57:44 AM
SW Download Task _14/02/...	Modify Release Config...	root	Stopped	Yes	Immediate	2014 Feb 11 09:40:09 AM
SW Download Task _14/02/...	Modify Release Config...	root	Stopped	Yes	Immediate	2014 Feb 20 04:16:42 PM
SW Download Task	Modify Release Config...	root	Stopped	Yes	Immediate	2014 Feb 11 09:30:16 AM
SW Download Task _14/02/...	Modify Release Config...	root	Stopped	Yes	Immediate	2014 Feb 11 01:16:53 PM
SW Download Task _14/02/...	Modify Release Config...	root	Stopped	Yes	Immediate	2014 Feb 10 12:03:03 PM
SW Download Task _14/02/...	Modify Release Config...	root	Stopped	Yes	Immediate	2014 Feb 11 08:56:19 AM
SW Download Task _14/02/...	Modify Release Config...	root	Stopped	Yes	Immediate	2014 Feb 11 08:43:13 AM
SW Download Task _13/12/...	Modify Release Config...	root	Stopped	Yes	Immediate	2013 Dec 20 03:27:22 PM

FIGURE 12-92 Task List Table

Click any column heading to sort the list by that column.

You can perform the following functions for a task:

- **View Details** - Open the Task Details Form for the task.
- **Start** - Execute the task.

- **Remove** - Delete the task.
- **Abort** - Stop the running task.
- **Cleanup** - Remove all tasks prior to a selected date.

12.4.4 Task Cleanup

You can clean up the Task List table by removing all tasks prior to a selected date. To clean up the Task List table:

1. From the main menu, go to **Tools > View Tasks**. The View Tasks window appears.
2. Click **Cleanup**.
3. In the **Task Cleanup** box, select the criteria date. All non-recurring tasks that have not been changed since that date will be selected. For example, if you select a criteria date of 2013 August 3, all tasks older than that date will be selected. A task that was last modified on 2013 August 9 will not be selected.
4. Click **Select**. The tasks that meet the criteria are selected in the Task List table.
5. Click **Remove** to remove the selected tasks from the table.

12.5 Other Device Control Tasks

12.5.1 Alarms/Events

Events and alarms indicate significant occurrences or changes on a monitored network that may be of interest to the Network Administrator. Events typically provide details on all significant occurrences on a monitored network. Alarms typically provide an indication of a condition or event that may require immediate attention. Right-clicking the device and choosing the *Alarms/Events* option will bring up the alarm and event views as follows:

- *Alarms* will bring up the Alarm panel with any alarms for the device.
- *Events* will bring up the Events Panel for the device.
- *Summary* will bring up a GUI showing the total and per-severity counts of events and alerts for the device.

12.5.2 Performance

Right-clicking the device and choosing the *Performance* menu option will bring up the Performance View (statistics) for the device.

12.5.3 File Comparison (Text Files)

The Configuration File Comparison feature compares and displays two **text** files side-by-side with their differences highlighted. Text files can be selected for comparison from the Configuration File Management, Command Script Management, and Device Backup/Restore applications. Any two text files from any two devices can be compared.

Note: This feature can only compare files that are created or part of Configuration File Management and Device Backup/Restore applications. Also, this feature does not compare binary files, so backup/restore files for iMAP devices cannot be compared. Configuration files, however, are in text format and can be compared. Finally, backup files are read-only, since they may be needed to reconfigure a device to a previous configuration.

This feature is most useful when comparing recurring backups, since changes between backups from the same device will be highlighted. Note that the comparison is between backup files, not the current configuration; to get a comparison between backup files and the current configuration, the user must back up the current configuration.

During backups, the latest configuration is automatically compared to the previous backup and if any changes are detected, the device's ConfigChanged property will be set to the time/date that the change was detected. Note that the change may have occurred at any time between the two backups.

The following table lists the scenarios where the File Comparison feature is used and the main steps that ar performed. Following this is an overview of the feature screens and examples.

TABLE 12-11 Scenarios for Text File Comparison

Task	Application	Steps
View Latest Changes	MAP device	1. User navigates to a map. 2. User right-clicks on a **single** supported device. 3. User selects **View Config Changes** from the menu. 4. The latest differing backup files for the device are displayed side-by-side with the differences highlighted. 5. The names, dates, and sizes of the files compared are also displayed.
View Latest Changes	Network Inventory	1. User navigates to the Network Inventory. 2. User right-clicks on a **single** supported device. 3. User selects **View Config Changes** from the menu. 4. The latest differing backup files for the device are displayed side-by-side with the differences highlighted. 5. The names, dates, and sizes of the files compared are also displayed.
View Latest Changes	Device Backup/ Restore	1. User navigates to Device Backup/Restore. 2. User right-clicks on a **single row**. 3. User selects the **Compare Files** button. 4. The latest differing backup files for the device are displayed side-by-side with their differences highlighted. 5. The names, dates, and sizes of the files compared are also displayed.
View Latest Changes	Config File Mgmt	1. User navigates to Config File Mgmt. 2. User right-clicks on a **single row**. 3. User selects the **Compare Files** button. 4. The latest differing config files for the device are displayed side-by-side with their differences highlighted. 5. The names, dates, and sizes of the files compared are also displayed.
View Changes	Device Backup/ Restore	1. User navigates to Device Backup/Restore. 2. User selects **Compare Files** button with **no rows** selected. 3. An empty comparison display pops up with fields for selecting/entering files. 4. User selects 2 files and then the **Diff** button. The file chooser defaults to the backup directory but also allows selecting files from the user's CCM directory. 5. The selected files are displayed side-by-side with their differences highlighted. 6. The names, dates, and sizes of the files are also displayed.

TABLE 12-11 Scenarios for Text File Comparison

Task	Application	Steps
View Changes	Config File Mgmt	1. User navigates to Config File Mgmt. 2. User selects **Compare Files** button with **no rows** selected. 3. An empty comparison display pops up with fields for selecting/entering files. 4. User selects 2 files and then the **Diff** button. The file chooser defaults to the user's CCM directory but also allows selecting files from the backup directory. 5. The selected files are displayed side-by-side with their differences highlighted. 6. The names, dates, and sizes of the files are also displayed.
View Changes	Command Script Mgmt	1. User navigates to Command Script Mgmt. 2. User selects **Compare Files** button **with or without rows selected**. 3. An empty comparison display pops up with fields for selecting/entering files. 4. User selects 2 files and then the Diff button. The file chooser defaults to the user's CCM directory but also allows selecting files from the backup directory. 5. The selected files are displayed side-by-side with their differences highlighted. 6. The names, dates, and sizes of the files are also displayed

12.5.3.1 Viewing Latest Config File Changes from MAP Device

Following is an example of the first scenario to show the screens and responses for viewing the latest changes.

For configuration comparison on a device, right click on the device and select View Config Changes. Refer to the following figure.

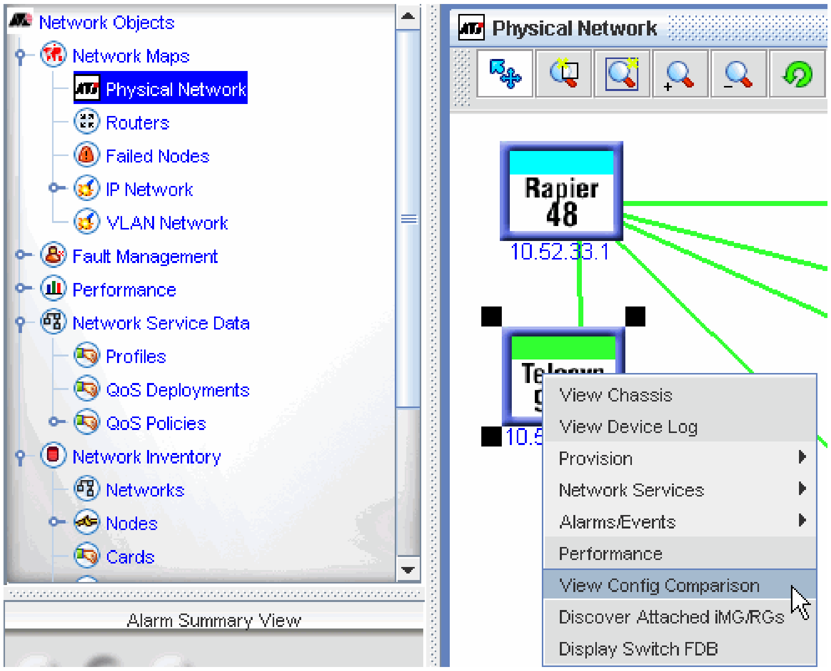
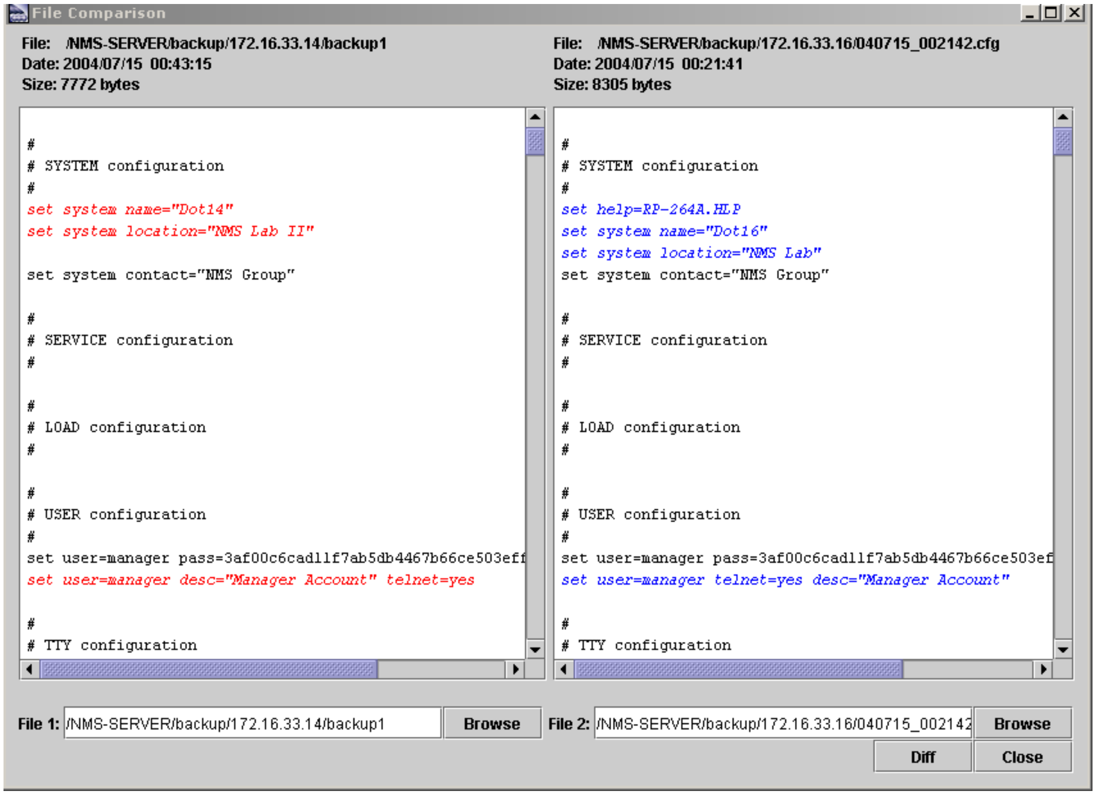


FIGURE 12-93 Selecting a Device for File Comparison

This will display the latest two text backup files from the selected device, side-by-side, with their differences highlighted. See the following figure.

Differences are indicated by highlighting text. Plain text shows lines that are the same in both files. Red text shows lines on the left which are not on the right while blue shows lines on the right which are not on the left. Missing lines are padded with blanks. If a line is simply modified, it shows up red on the left and blue on the right. Extra lines on the left are red and corresponding lines on the right are padded with blanks. Extra lines on the right are blue and corresponding lines on the left are padded with blanks.



File: /NMS-SERVER/backup/172.16.33.14/backup1
Date: 2004/07/15 00:43:15
Size: 7772 bytes

```
#
# SYSTEM configuration
#
set system name="Dot14"
set system location="NMS Lab II"

set system contact="NMS Group"

#
# SERVICE configuration
#

#
# LOAD configuration
#

#
# USER configuration
#
set user=manager pass=3af00c6cad11f7ab5db4467b66ce503eff
set user=manager desc="Manager Account" telnet=yes

#
# TTY configuration
```

File: /NMS-SERVER/backup/172.16.33.16/040715_002142.cfg
Date: 2004/07/15 00:21:41
Size: 8305 bytes

```
#
# SYSTEM configuration
#
set help=RP-264A.HLP
set system name="Dot16"
set system location="NMS Lab"
set system contact="NMS Group"

#
# SERVICE configuration
#

#
# LOAD configuration
#

#
# USER configuration
#
set user=manager pass=3af00c6cad11f7ab5db4467b66ce503ef
set user=manager telnet=yes desc="Manager Account"

#
# TTY configuration
```

File 1: /NMS-SERVER/backup/172.16.33.14/backup1

File 2: /NMS-SERVER/backup/172.16.33.16/040715_002142

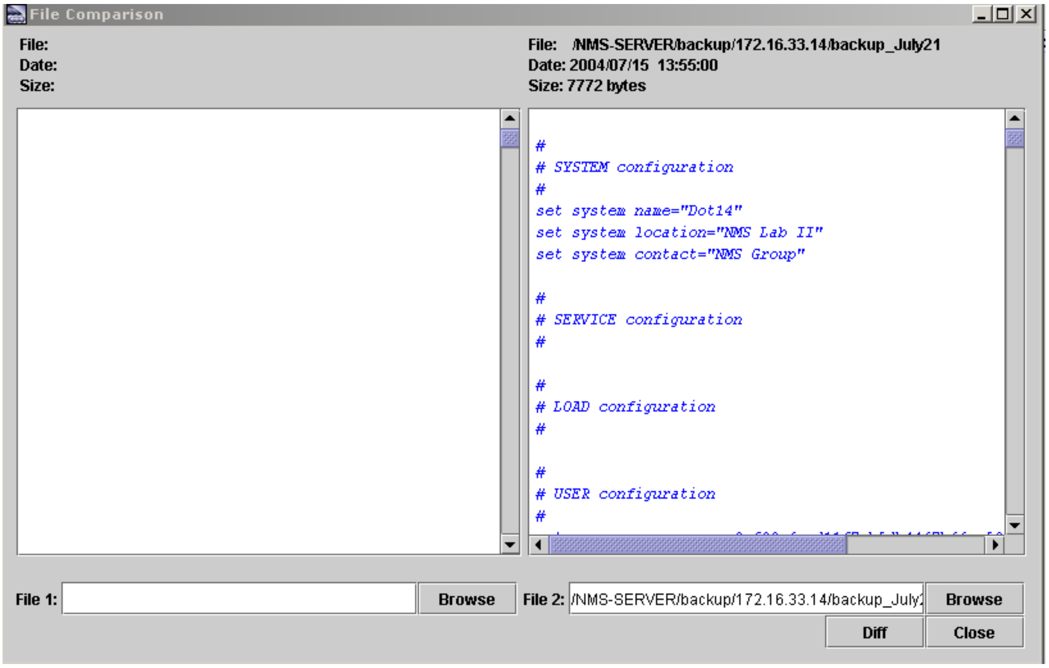
FIGURE 12-94 Comparing Two Backup Files - Highlighting of Differences

If there are multiple backup files that are identical, the **latest two that are different** will be displayed.

Only one file is displayed with the other window blank if:

- All backup files are identical.
- There is only one backup file.

Refer to the following figure.



File:
Date:
Size:

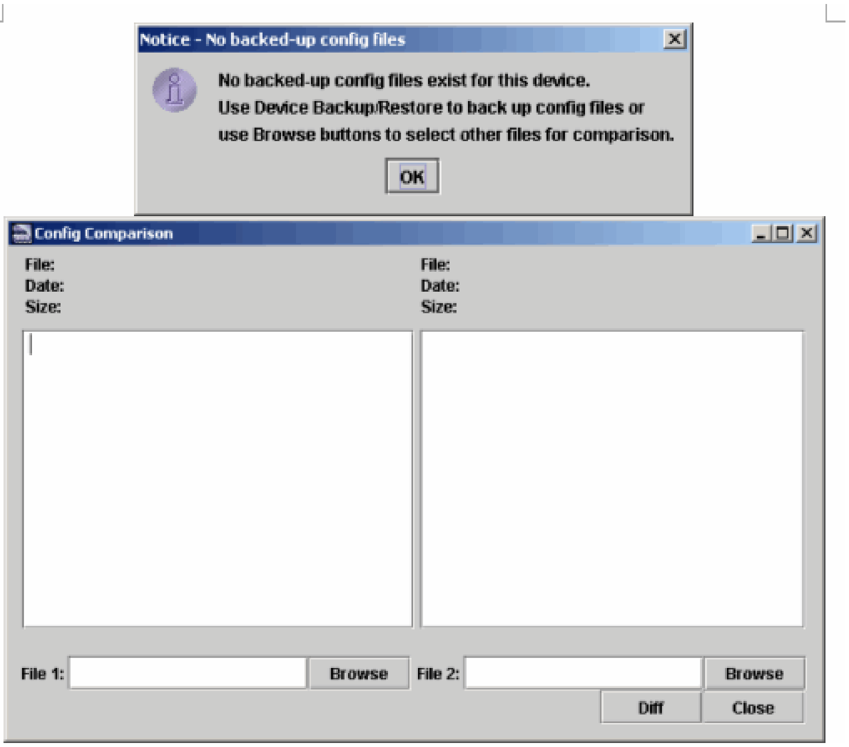
File: /NMS-SERVER/backup/172.16.33.14/backup_July21
Date: 2004/07/15 13:55:00
Size: 7772 bytes

```
#
# SYSTEM configuration
#
set system name="Dot14"
set system location="NMS Lab II"
set system contact="NMS Group"

#
# SERVICE configuration
#

#
# LOAD configuration
#

#
# USER configuration
#
```

File 1:
File 2: /NMS-SERVER/backup/172.16.33.14/backup_July2

FIGURE 12-95 Only One Backup file - No Comparison Possible

If there are no backup files, and the display will be empty and a notice will pop up indicating no backup files exist for the device. See the following figure.



No backed-up config files exist for this device.
Use Device Backup/Restore to back up config files or
use Browse buttons to select other files for comparison.

File:
Date:
Size:

File:
Date:
Size:

File 1:
File 2:

FIGURE 12-96 No Files Available for Comparison

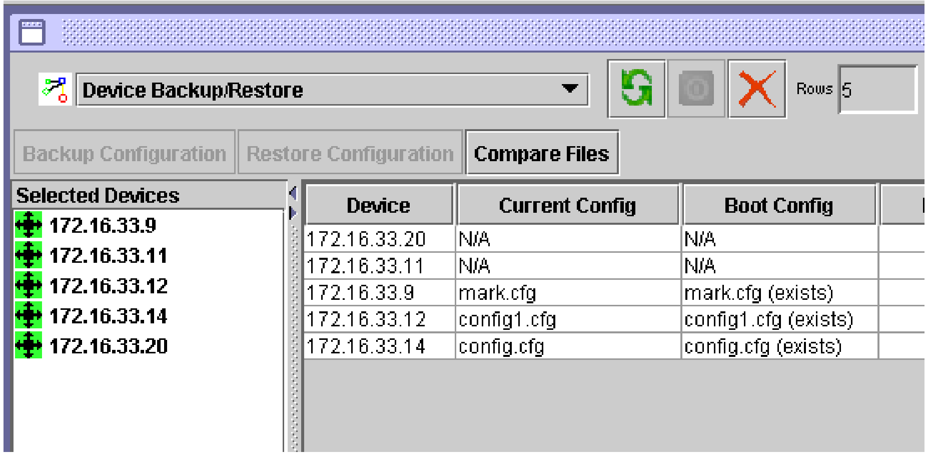
At the top of the display are the file names, their dates, and their sizes. These are updated whenever the files are compared, so they always indicate exactly which files are being compared.

When the user enters other files into the file-selection boxes at the bottom of the display (explained below), they will not take effect until the **Diff** button is pushed. Therefore the bottom file names may not match the displayed data.

Note: If the devices are set to create backups on a schedule, a large number of backup files may be created. The administrator should check the backup/device directories and delete any files that are not needed.

12.5.3.2 Other Applications

The **Compare Files** button on the Device Backup/Restore, Command Script Mgmt, and Config File Mgmt screens can also be used to bring up the differences display. The following figure shows the button



Selected Devices
172.16.33.9
172.16.33.11
172.16.33.12
172.16.33.14
172.16.33.20

Device	Current Config	Boot Config
172.16.33.20	N/A	N/A
172.16.33.11	N/A	N/A
172.16.33.9	mark.cfg	mark.cfg (exists)
172.16.33.12	config1.cfg	config1.cfg (exists)
172.16.33.14	config.cfg	config.cfg (exists)

FIGURE 12-97 Compare Files Panel

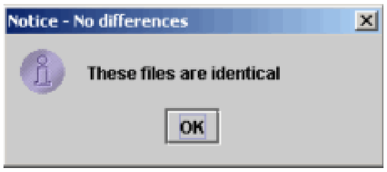
- If a row is selected from the **Device Backup/Restore** application, the dialog will be pre-filled with the 2 most recent different backup files, if any-as if the device were selected from a map or the network inventory. Note that the backup files are read-only, since these must not be edited in case they are needed.
- If a row is selected from the **Config File Mgmt** screen, the dialog will be pre-filled with the 2 most recent config files from the user's CCM directory, if any.
- For the **Command Script Mgmt** screen, the dialog box comes up empty. Whether the dialog is pre-filled or not, other files can be selected for comparison after the dialog is up. Any number of dialogs can be up at the same time.

Note: For these scenarios, the dialog title is File Comparison rather than Config Comparison.

12.5.3.3 Error Messages

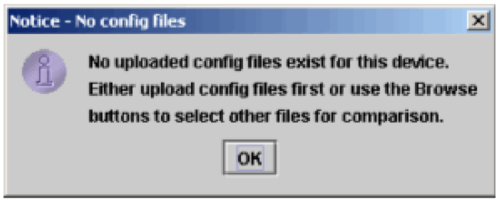
Some miscellaneous error messages and notices include the following:

- Files are identical - When two files compared are actually identical, they are both displayed side-by-side in regular fonts. This notice pops up, too since it may not be immediately obvious that they are identical.



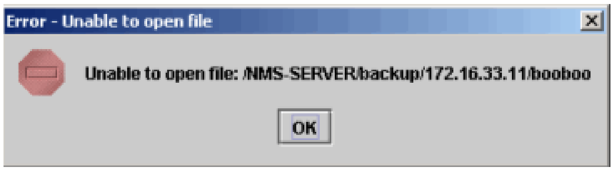
These files are identical

- No files found in user’s subdirectory - When brought up from Config File Management, config files are searched for in the user's config file subdirectory instead of the backup directory. This message is displayed if no files are found for the device in the user's subdirectory.



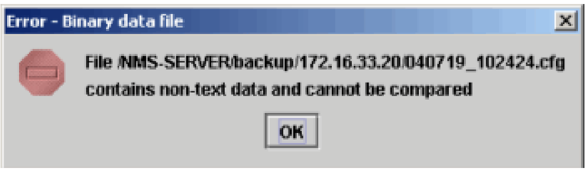
No uploaded config files exist for this device. Either upload config files first or use the Browse buttons to select other files for comparison.

- File not found



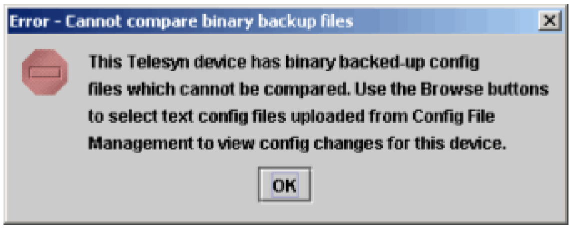
Unable to open file: /NMS-SERVER/backup/172.16.33.11/booboo

- Rejection of binary file - This application has made a best effort to recognize and then reject binary files which are not valid for text file comparison.



File /NMS-SERVER/backup/172.16.33.20/040719_102424.cfg contains non-text data and cannot be compared

- Device Backup/Restore stores iMAP configurations as binary databases - These files are not valid for text file comparison. Config File Mgmt, however, can upload text config files for iMAP devices starting at release 3.0 and these files are available for text file comparison, however Config File Mgmt does not provide recurrent backups, so each file has to be uploaded on demand.

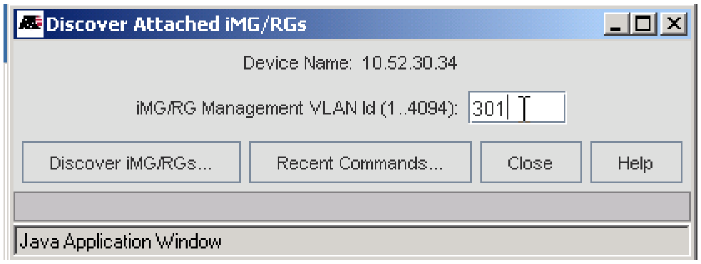


This Telesyn device has binary backed-up config files which cannot be compared. Use the Browse buttons to select text config files uploaded from Config File Management to view config changes for this device.

12.5.4 Discover Attached iMG/RGs

For a detailed explanation of how DHCP is set up so that iMG/RGs can be discovered and configured, refer to "Configuring Components for DHCP Discovery" on page 765. On initial discovery of the iMG/RG (out of the box or provisioned to a different Access Island), the bootstrap VLAN is used. Subsequent discoveries are performed using the RGMgmt VLAN.

This option will (re)discover **all** the iMGs/RGs attached to the iMAP device that use the RGMgmt VLAN. Refer to the following figure.



Device Name: 10.52.30.34

iMG/RG Management VLAN Id (1..4094): 301

FIGURE 12-98 Discover iMG/RGs for a Device over RGMgmt VLAN

Using this option allows the administrator to perform the discovery immediately and not have to wait for the 24-hour Discovery interval. Any changes made to the iMG/RG, such as profile changes, will be made and reflected in the iMG/RG node in the Network Inventory view as well as the **Triple Play Service Management** Form.

Note: *The user can also right click on an individual iMG/RG and perform a rediscovery using the RGMgmt VLAN.*

Note: *For iMGs attached to AlliedWare Plus devices, iMGs will be discovered as long their management IPs haven't aged out of the router's ARP table. In the rare case where the ARP table has not been refreshed, you can use Add Network to rediscover all of the iMGs, or Add Node to discover by specific IP(s).*

12.5.5 Display Switch Forwarding Database (iMAP Systems)

To view the switch forwarding entries for iMAP devices there is the option Display Switch FDB, accessed by:

- Right clicking on an iMAP physical icon or a node in the inventory table
- Selecting an iMAP physical icon or a node in the inventory table and then accessing the Operations pull-down menu

The Switch Forwarding Database window appears, and includes the Port, VLAN ID, MAC Address, and Status.

Note: *This is the same output as the SHOW SWITCH FDB command from the device's CLI.*

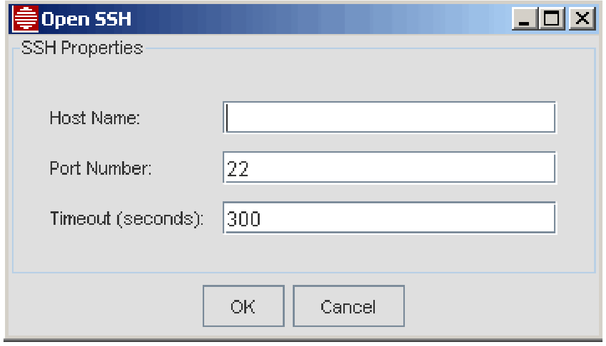
12.5.6 Telnet / SSH to a Device

To access a device using telnet or SSH, there are the following options.

12.5.6.1 Access a Telnet or SSH-enabled Device

Use *Tools -> Open Telnet* or *Tools-> Open SSH* to connect to any device that is telnet- or SSH-enabled and is accessible.

Refer to the following figure that is used for SSH-enabled devices.



Host Name:

Port Number: 22

Timeout (seconds): 300

FIGURE 12-99 Accessing a Device for SSH

Note: *For SSH, the user-specified Time-out is ignored. If the connection fails to establish, manually close the window.*

Note: *For Telnet, changing the Timeout value when accessing a device sets the value for other devices as well, so if you right click on the device and select 'Telnet to Device' it will have the timeout value that you set.*

12.5.6.2 Access a Discovered Device

Right-clicking the device and choosing the *Telnet To Device* option brings up a command line window with a login prompt for a telnet session, allowing you to send commands directly to the device.

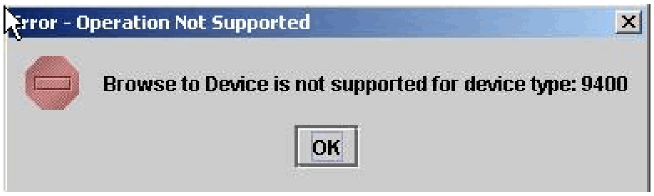
Right-clicking the device and choosing the *SSH To Device* option brings up a panel to fill in the User name and Password. If the device supports SSH and has been configured for SSH, the correct user name and password will access to the device.

Note: *The SSH session for iMG/iBG's only accepts one user at a time. So if an active connection is established by the NMS, the "SSH to Device" and "Open SSH" function won't work for these device families.*

12.5.7 Browse Device (Rapier Device Only)

To access the Web-enabled on-device management GUI, right-click the device and choose *Browse Device*.

The Browse Device feature is not currently supported for iMAP devices. If an iMAP device is chosen, the following example window appears.



Error - Operation Not Supported

Browse to Device is not supported for device type: 9400

12.5.8 Rediscovery Device (When Required)

This option picks up any changes made to the selected device. This action is most commonly done in the following scenarios:

- The user has updated the user/password in the Managed Objects properties form and wishes to activate the changes.
- A login to a device fails, an alarm is generated, and the user updates the login-password in the manager properties form. The user then clicks on **Rediscover Device** to retry the device discovery with the newly entered userid/password. If the discovery succeeds the alarm is cleared.
- Cards on the device have been re configured. A manual rediscovery is necessary to ensure alarms/conditions are correctly reported (i.e. correct card or port).

Note: If the user does not do a manual rediscovery, the 24-hour rediscovery will be performed and will pick up the changes.

Caution: When changes to a device configuration are made directly on the device (using the CLI) rather than using the NMS, the NMS data will be out of sync with the device, and must be put back in sync by either the 24-hour audit or manual rediscovery.

Caution: The name for a device should not include an '&' or Rediscovery will fail.

12.5.9 Managed Object Properties

To view the Object Properties of a either a Rapier or iMAP device, right click on the device and select *Managed Object Properties*. The Managed Object Properties Form appears.

12.5.10 Manage/Unmanage

To toggle between having the AlliedView NMS monitor the device choose *UnManage* (or if the device is not being managed, *Manage*). This will repoll the device and updated all related information.

12.5.11 Update Status

To poll the device and update the status of the managed object, select *Operations -> Update Status.* Device status is normally polled automatically by the NMS at the poll interval set in each device's Managed Object Properties. The Update Status operation lets the user initiate a status poll outside the normal interval. Status is determined according to the Tester property of each device's Managed Object Properties. Valid values for Tester are:

- Ping - The device is polled merely by pinging it with ICMP.
- Snmpping - A more detailed poll is made using snmp.
- Max - The device's status is rolled-up from the current status of all its components in the database, however they were determined (which themselves may have been ping, snmpping, or max), without actually going to the device. Thus with max, a router's status would be the maximum status of all its interfaces.

12.6 Manage CLI Users

Note: This option is available only to users in the Admin group and is part of the Discovery panel.

This option is used to specify common CLI login-passwords for a set of devices. This data is then used during the discovery process to log in on each device and save the username/password pair on a per-device basis.

12.7 Customer Cutover

Customer cutover is an automated port deprovisioning and reprovisioning process that transfers all parameter settings from one port to another. iMAP device (if using another chassis), slot and customer port ID change, but all other port parameter settings remain the same.

Cases for customer cutover include:

- Port failure
- Network reorganization
- Card upgrades

You can migrate a customer from one port to another on the same card, to a port on another card in the same chassis, or to a port on another card in a different chassis. You can use customer cutover to move customers to an upgraded card. During ADSL and SHDSL card upgrades, for example, all the customers from one card can be migrated to an upgraded card, such as going from an ADSL16 card to an ADSL24 or ADSL48 card.

12.7.1 Supported Cards

Table 12-12 lists the cards that support customer cutover.

TABLE 12-12 **Customer Cutover Supported Cards**

Interface Type	Card Type	Notes
ADSL	ADSL8S ADSL16 ADSL16B ADSL16C ADSL24 ADSL24A/B ADSL48A/B ADSL48B ADSL24AE	The annex of the destination card must match the source card for all ADSL and VDSL cards. The NMS does not validate matching annexes for the non-annexed version of the ADSL24 card.
FE	FE10	
FX	FX10, FX20	FX10 and FX20 cards support customer cutover to the GE24BX and GE24SFP cards. See "FX to GE" on page 354.

TABLE 12-12 Customer Cutover Supported Cards

Interface Type	Card Type	Notes
GE	GE3 GE8 GE24SFP GE2RJ GE4 GE24BX GE24POE	GE3 is supported for the network direction only.
SHDSL	SHDSL16 SHDSL24	Bonded ports must be moved together to a congruent pair of destination ports.
VDSL	VDSL24A VDSL24B	The annex of the destination card must match the source card for all ADSL and VDSL cards.

12.7.2 Restrictions

The following restrictions apply:

- Only provisioned ports can be cut over.
- Customer cutover involves interaction, and cannot be scheduled or executed from a task.
- You cannot cut over interface types with non-transferable or context-sensitive parameter settings. Interfaces of this type include:
  - CES ports, which depend on card IP configuration and PSPAN configuration
  - NTE ports, which depend on PPP and DS1/DS0 configuration
  - POTS ports
- You can only cut over ports of the same interface type, such as ADSL to ADSL, to ensure source port parameter settings map to destination port parameter settings.
- To ensure parameter compatibility, customer cutover is restricted to destination ports on devices running the same or higher version of software as the source device, and for ADSL and VDSL, the same annex (A, B, or C).
- When the new ports are provisioned, they are initially provisioned with the port profile. This ensures the creation of classifiers as well as parameters that may not be present on the source card and are introduced by an upgraded card.
- The cutover must occur within the same Access Island. The NMS assumes the VLAN configuration is unchanged.

12.7.3 Overview of the Customer Cutover Procedure

The order of events for customer cutover is:

1. A hardware technician performs the necessary changes on the hardware.
2. The NMS operator prepares the configuration changes in the NMS.
3. When the hardware change is complete, the NMS operator invokes the cutover and tests the configuration.
4. When testing is complete, the NMS operator de-provisions the previous customer configurations.
5. A hardware technician removes any hardware that is no longer needed.

To perform customer cutover, use the **Port Management** screen to specify one or more source ports on the source card and one or more destination ports on the destination card. The NMS cuts over the ports, ensuring all parameter settings are maintained between the source and destination ports. Once the cutover is complete the NMS database and related components reflect the changes.

The customer cutover procedure involves the following steps:

- Open the **Port Management** screen.
- Select the source ports.
- Select the destination ports. All destination ports must be on the same device.
- Provision the new ports.
- Deprovision the old ports.

The NMS automatically restricts destination ports to ones that are compatible with the selected source ports. In some cases, the NMS assigns default destination ports. You can change these if necessary.

Once you provision the new ports they are enabled for testing. When testing is complete you can deprovision the old ports immediately or deprovision them at a later time from the **Port Management** screen.

12.7.4 FX to GE

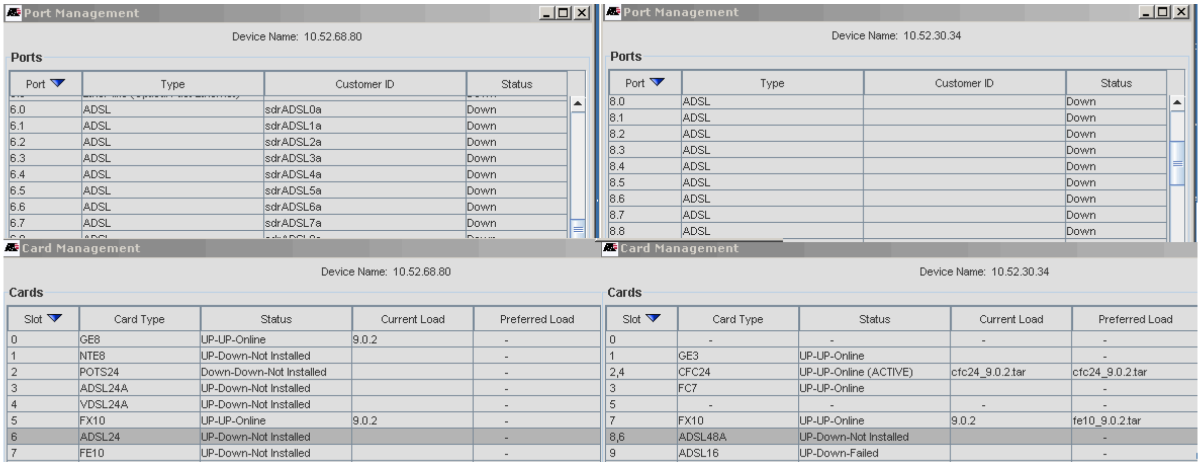
The NMS supports customer cutover from FX10 or FX20 cards to either the GE24BX card on iMAP devices or the GE24SFP card on SBx3100 devices. When you cut over an iMG from an FX to a GE card, the iMG may or may not support the 1000 Mbps speed the GE card supports (depending on the iMG). To minimize potential iMG downtime in case the iMG does not support the higher speed, the NMS ignores the port profile and automatically sets the following parameters on GE interfaces during the cutover:

- autonegotiation=OFF
- speed=100Mbps
- duplex=FULL

If these settings do not match the port profile for the GE interfaces, the next time the NMS discovers the device it flags the settings as mismatched. To modify the settings after the cutover, you can reapply the port profile or view the device and modify the settings.

12.7.5 Example: Transferring Customers From One Card to Another

This example demonstrates how to transfer customers on the 24 ports of an ADSL24 card to the ports on an ADSL48A card. Figure 12-100 shows the initial configuration for the source and destination devices on the **Port Management** and **Card Management** screens. **10.52.60.80** is the source iMAP device and **10.52.30.34** is the destination iMAP device.



Device Name: 10.52.68.80

Port	Type	Customer ID	Status
6.0	ADSL	sdrADSL0a	Down
6.1	ADSL	sdrADSL1a	Down
6.2	ADSL	sdrADSL2a	Down
6.3	ADSL	sdrADSL3a	Down
6.4	ADSL	sdrADSL4a	Down
6.5	ADSL	sdrADSL5a	Down
6.6	ADSL	sdrADSL6a	Down
6.7	ADSL	sdrADSL7a	Down

Device Name: 10.52.30.34

Port	Type	Customer ID	Status
8.0	ADSL		Down
8.1	ADSL		Down
8.2	ADSL		Down
8.3	ADSL		Down
8.4	ADSL		Down
8.5	ADSL		Down
8.6	ADSL		Down
8.7	ADSL		Down
8.8	ADSL		Down

Device Name: 10.52.68.80

Slot	Card Type	Status	Current Load	Preferred Load
0	GE8	UP-UP-Online	9.0.2	-
1	NTE8	UP-Down-Not Installed		-
2	POTS24	Down-Down-Not Installed		-
3	ADSL24A	UP-Down-Not Installed		-
4	VDSL24A	UP-Down-Not Installed		-
5	FX10	UP-UP-Online	9.0.2	-
6	ADSL24	UP-Down-Not Installed		-
7	FE10	UP-Down-Not Installed		-

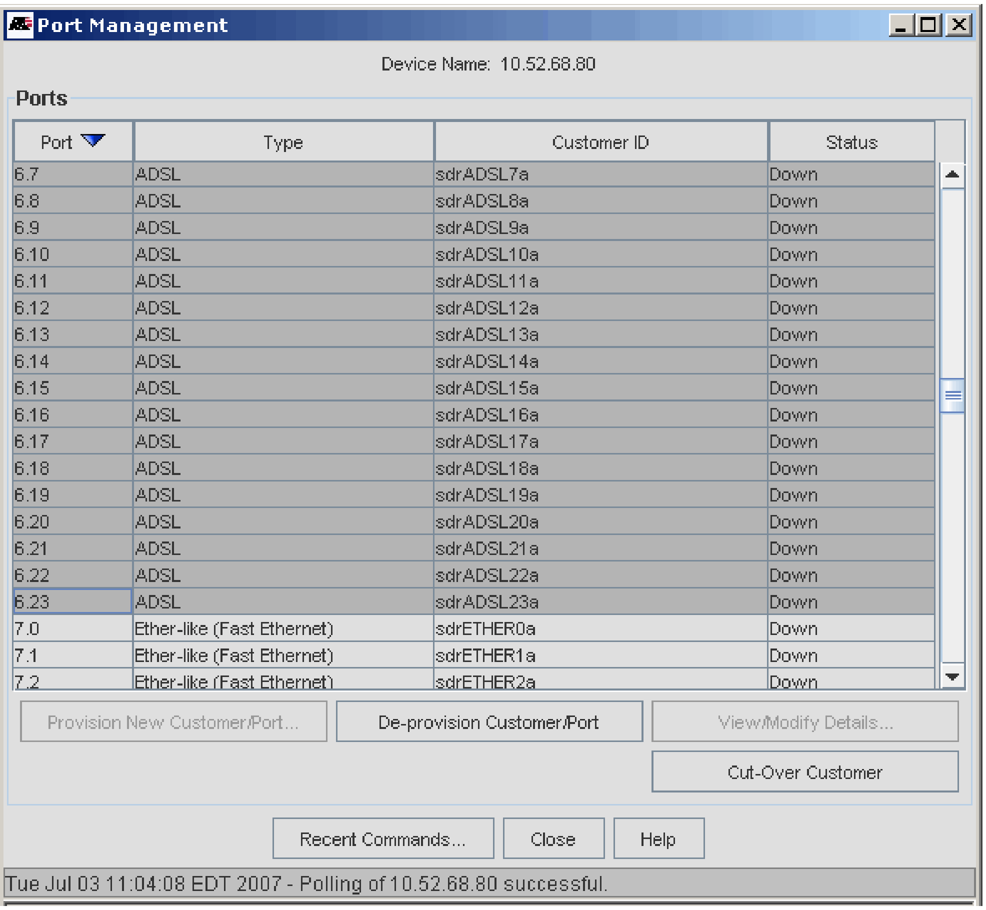
Device Name: 10.52.30.34

Slot	Card Type	Status	Current Load	Preferred Load
0	-	-	-	-
1	GE3	UP-UP-Online		-
2,4	CFC24	UP-UP-Online (ACTIVE)	cfc24_9.0.2.tar	cfc24_9.0.2.tar
3	FC7	UP-UP-Online		-
5	-	-	-	-
7	FX10	UP-UP-Online	9.0.2	fe10_9.0.2.tar
8,6	ADSL48A	UP-Down-Not Installed		-
9	ADSL16	UP-Down-Failed		-

FIGURE 12-100 Customer Cutover - Initial Configuration

To transfer customers from one card to another:

1. Do one of the following in the **Network Objects** panel:
   - Go to **Network Maps** > **Physical Network**. In the **Physical Network** screen, select the device.
   - Go to **Network Inventory** > **Nodes**. In the **Nodes** screen, select the device.
2. Go to **Operations** > **Provision** > **Port Management**. The **Port Management** window appears.
3. Select the source device the ports to cut over. In most cases these will be contiguous ports on a card.



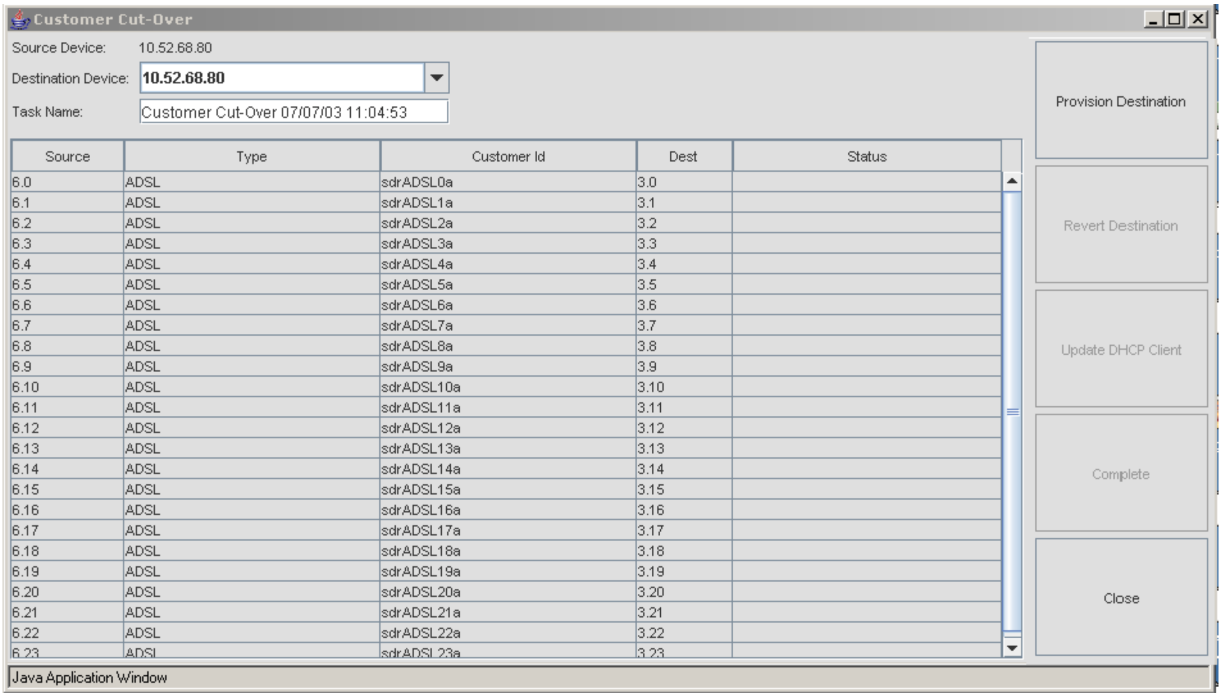
Device Name: 10.52.68.80

Port	Type	Customer ID	Status
6.7	ADSL	sdrADSL7a	Down
6.8	ADSL	sdrADSL8a	Down
6.9	ADSL	sdrADSL9a	Down
6.10	ADSL	sdrADSL10a	Down
6.11	ADSL	sdrADSL11a	Down
6.12	ADSL	sdrADSL12a	Down
6.13	ADSL	sdrADSL13a	Down
6.14	ADSL	sdrADSL14a	Down
6.15	ADSL	sdrADSL15a	Down
6.16	ADSL	sdrADSL16a	Down
6.17	ADSL	sdrADSL17a	Down
6.18	ADSL	sdrADSL18a	Down
6.19	ADSL	sdrADSL19a	Down
6.20	ADSL	sdrADSL20a	Down
6.21	ADSL	sdrADSL21a	Down
6.22	ADSL	sdrADSL22a	Down
6.23	ADSL	sdrADSL23a	Down
7.0	Ether-like (Fast Ethernet)	sdrETHER0a	Down
7.1	Ether-like (Fast Ethernet)	sdrETHER1a	Down
7.2	Ether-like (Fast Ethernet)	sdrETHER2a	Down

Tue Jul 03 11:04:08 EDT 2007 - Polling of 10.52.68.80 successful.

FIGURE 12-101 Selecting Source Ports

4. Click **Cut-Over Customer**. The **Customer Cut-Over** screen appears.



Source Device: 10.52.68.80

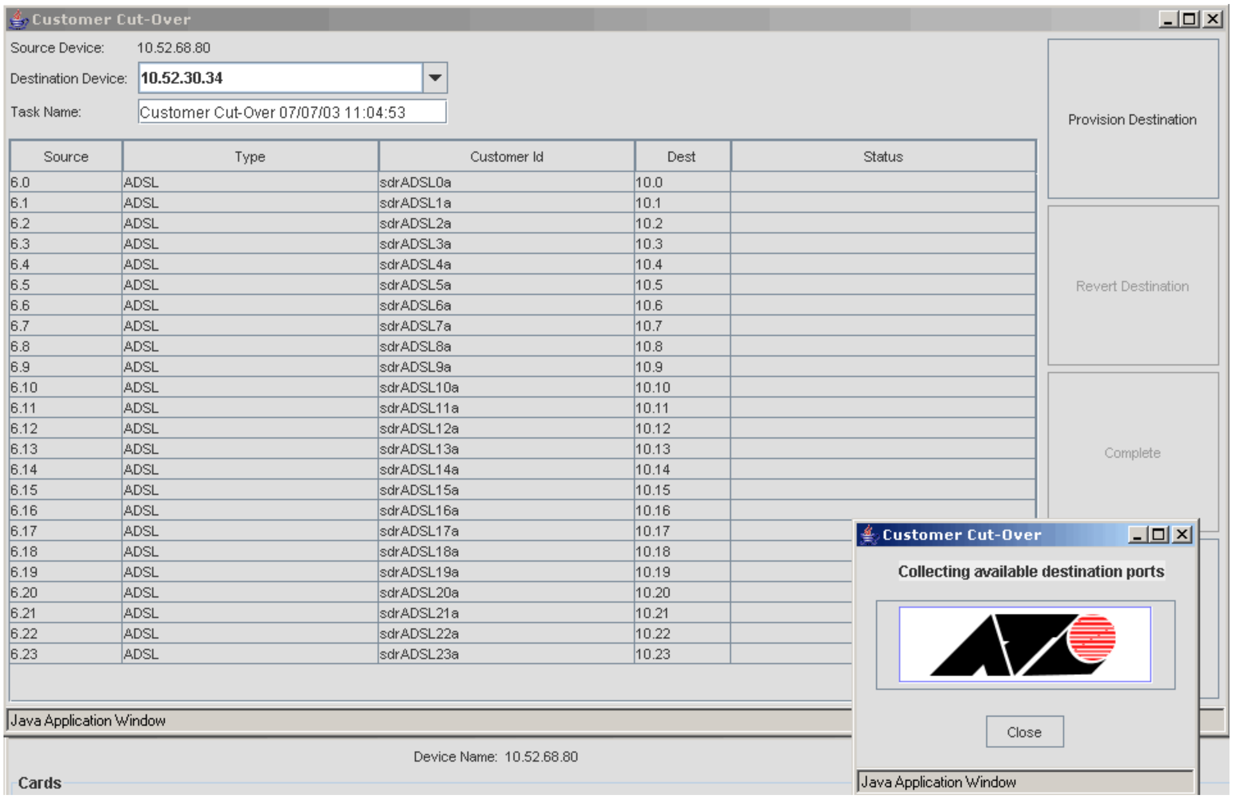
Destination Device: 10.52.68.80

Task Name: Customer Cut-Over 07/07/03 11:04:53

Source	Type	Customer Id	Dest	Status
6.0	ADSL	sdrADSL0a	3.0	
6.1	ADSL	sdrADSL1a	3.1	
6.2	ADSL	sdrADSL2a	3.2	
6.3	ADSL	sdrADSL3a	3.3	
6.4	ADSL	sdrADSL4a	3.4	
6.5	ADSL	sdrADSL5a	3.5	
6.6	ADSL	sdrADSL6a	3.6	
6.7	ADSL	sdrADSL7a	3.7	
6.8	ADSL	sdrADSL8a	3.8	
6.9	ADSL	sdrADSL9a	3.9	
6.10	ADSL	sdrADSL10a	3.10	
6.11	ADSL	sdrADSL11a	3.11	
6.12	ADSL	sdrADSL12a	3.12	
6.13	ADSL	sdrADSL13a	3.13	
6.14	ADSL	sdrADSL14a	3.14	
6.15	ADSL	sdrADSL15a	3.15	
6.16	ADSL	sdrADSL16a	3.16	
6.17	ADSL	sdrADSL17a	3.17	
6.18	ADSL	sdrADSL18a	3.18	
6.19	ADSL	sdrADSL19a	3.19	
6.20	ADSL	sdrADSL20a	3.20	
6.21	ADSL	sdrADSL21a	3.21	
6.22	ADSL	sdrADSL22a	3.22	
6.23	ADSL	sdrADSL23a	3.23	

FIGURE 12-102 Customer Cut-Over Screen

5. In the **Destination Device** drop-down list, select **10.52.30.34**. The available destination ports are displayed.



Source Device: 10.52.68.80

Destination Device: 10.52.30.34

Task Name: Customer Cut-Over 07/07/03 11:04:53

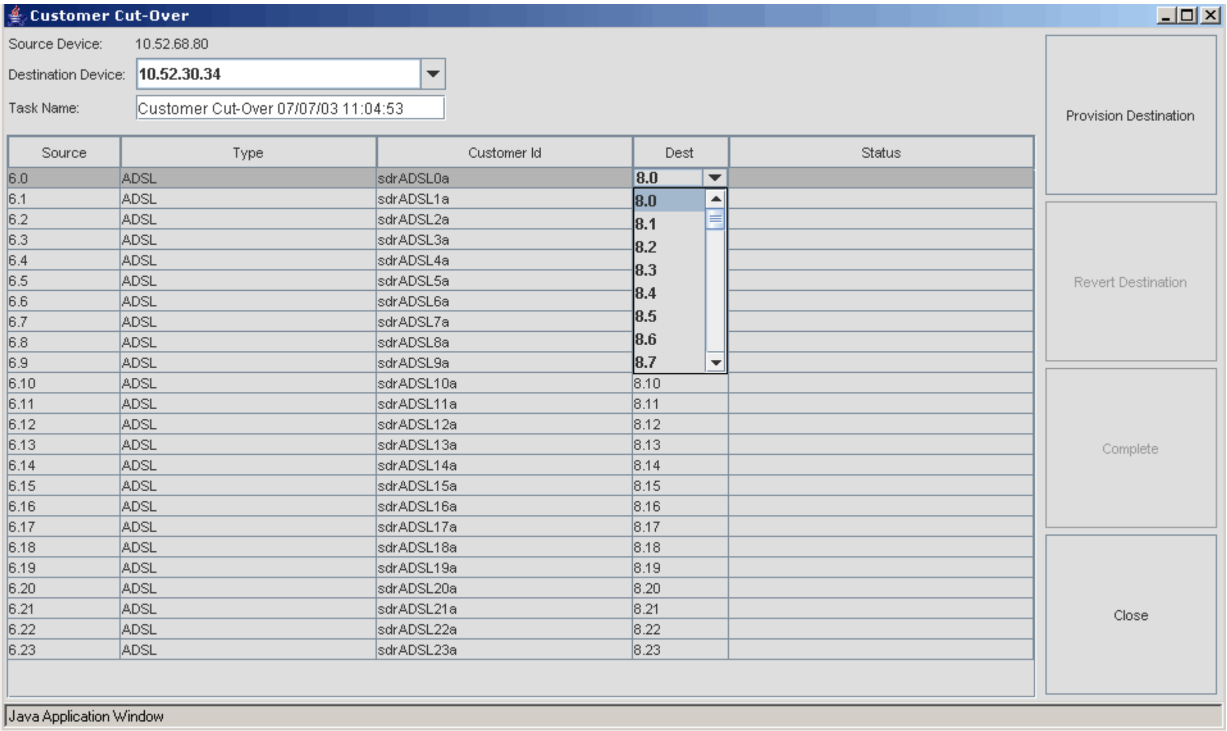
Source	Type	Customer Id	Dest	Status
6.0	ADSL	sdrADSL0a	10.0	
6.1	ADSL	sdrADSL1a	10.1	
6.2	ADSL	sdrADSL2a	10.2	
6.3	ADSL	sdrADSL3a	10.3	
6.4	ADSL	sdrADSL4a	10.4	
6.5	ADSL	sdrADSL5a	10.5	
6.6	ADSL	sdrADSL6a	10.6	
6.7	ADSL	sdrADSL7a	10.7	
6.8	ADSL	sdrADSL8a	10.8	
6.9	ADSL	sdrADSL9a	10.9	
6.10	ADSL	sdrADSL10a	10.10	
6.11	ADSL	sdrADSL11a	10.11	
6.12	ADSL	sdrADSL12a	10.12	
6.13	ADSL	sdrADSL13a	10.13	
6.14	ADSL	sdrADSL14a	10.14	
6.15	ADSL	sdrADSL15a	10.15	
6.16	ADSL	sdrADSL16a	10.16	
6.17	ADSL	sdrADSL17a	10.17	
6.18	ADSL	sdrADSL18a	10.18	
6.19	ADSL	sdrADSL19a	10.19	
6.20	ADSL	sdrADSL20a	10.20	
6.21	ADSL	sdrADSL21a	10.21	
6.22	ADSL	sdrADSL22a	10.22	
6.23	ADSL	sdrADSL23a	10.23	

Collecting available destination ports

Device Name: 10.52.68.80

FIGURE 12-103 Destination Ports

6. The **Dest** column lists the destination ports. If the default port is not the correct port, select the port in the **Dest** column, then select a new port from the drop-down list.



Source Device: 10.52.68.80

Destination Device: 10.52.30.34

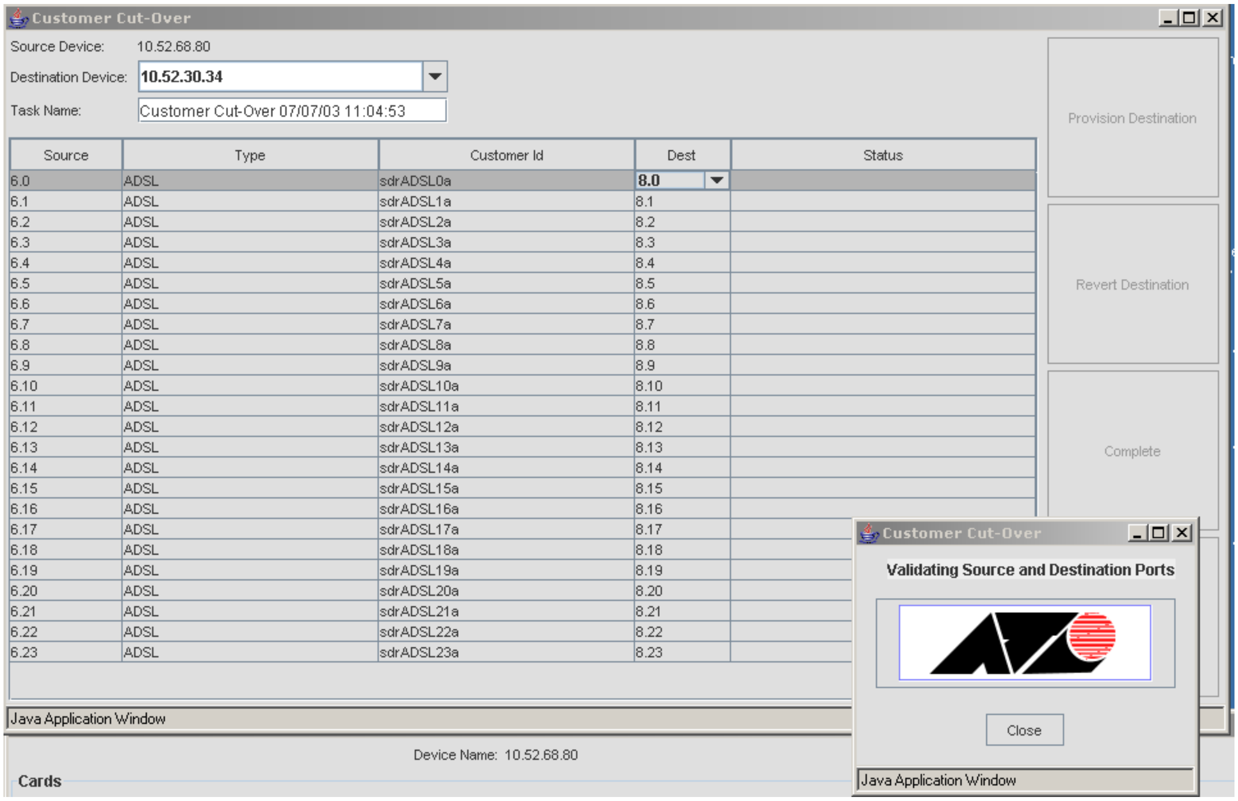
Task Name: Customer Cut-Over 07/07/03 11:04:53

Source	Type	Customer Id	Dest	Status
6.0	ADSL	sdrADSL0a	8.0	
6.1	ADSL	sdrADSL1a		
6.2	ADSL	sdrADSL2a		
6.3	ADSL	sdrADSL3a		
6.4	ADSL	sdrADSL4a		
6.5	ADSL	sdrADSL5a		
6.6	ADSL	sdrADSL6a		
6.7	ADSL	sdrADSL7a		
6.8	ADSL	sdrADSL8a		
6.9	ADSL	sdrADSL9a		
6.10	ADSL	sdrADSL10a	8.10	
6.11	ADSL	sdrADSL11a	8.11	
6.12	ADSL	sdrADSL12a	8.12	
6.13	ADSL	sdrADSL13a	8.13	
6.14	ADSL	sdrADSL14a	8.14	
6.15	ADSL	sdrADSL15a	8.15	
6.16	ADSL	sdrADSL16a	8.16	
6.17	ADSL	sdrADSL17a	8.17	
6.18	ADSL	sdrADSL18a	8.18	
6.19	ADSL	sdrADSL19a	8.19	
6.20	ADSL	sdrADSL20a	8.20	
6.21	ADSL	sdrADSL21a	8.21	
6.22	ADSL	sdrADSL22a	8.22	
6.23	ADSL	sdrADSL23a	8.23	

FIGURE 12-104 Ability to Choose any Valid Destination Port

Note: *Although the destination ports are valid since they are the same type, the NMS will produce an error message if the user tries to transfer an Annexed port to a non-Annexed port.*

7. Click **Provision Destination**. The NMS validates the the source and destination ports and displays the status of the transfer as the task completes.



Source Device: 10.52.68.80

Destination Device: 10.52.30.34

Task Name: Customer Cut-Over 07/07/03 11:04:53

Source	Type	Customer Id	Dest	Status
6.0	ADSL	sdrADSL0a	8.0	
6.1	ADSL	sdrADSL1a	8.1	
6.2	ADSL	sdrADSL2a	8.2	
6.3	ADSL	sdrADSL3a	8.3	
6.4	ADSL	sdrADSL4a	8.4	
6.5	ADSL	sdrADSL5a	8.5	
6.6	ADSL	sdrADSL6a	8.6	
6.7	ADSL	sdrADSL7a	8.7	
6.8	ADSL	sdrADSL8a	8.8	
6.9	ADSL	sdrADSL9a	8.9	
6.10	ADSL	sdrADSL10a	8.10	
6.11	ADSL	sdrADSL11a	8.11	
6.12	ADSL	sdrADSL12a	8.12	
6.13	ADSL	sdrADSL13a	8.13	
6.14	ADSL	sdrADSL14a	8.14	
6.15	ADSL	sdrADSL15a	8.15	
6.16	ADSL	sdrADSL16a	8.16	
6.17	ADSL	sdrADSL17a	8.17	
6.18	ADSL	sdrADSL18a	8.18	
6.19	ADSL	sdrADSL19a	8.19	
6.20	ADSL	sdrADSL20a	8.20	
6.21	ADSL	sdrADSL21a	8.21	
6.22	ADSL	sdrADSL22a	8.22	
6.23	ADSL	sdrADSL23a	8.23	

Validating Source and Destination Ports

Device Name: 10.52.68.80

Cards

FIGURE 12-105 Provisioning the Destination Ports

8. Disconnect the ADSL cables from the ADSL24 card and connect them to the ADSL48 card.

Note: You may need to change cabling facilities to connect the ADSL cables to another card. Refer to the iMAP Component Specification for information on ADSL cabling types.

The ports are now active and are physically connected to the iMGs. If the iMGs are successfully connected to the destination ports, they must renew their IP addresses (if assigned using DHCP) to update DHCP-based filtering on the iMAP ports.

9. Check connectivity with the iMGs. If connectivity fails, proceed to step 10. Otherwise, proceed to step 11.
10. If the iMGs are still powered on and connectivity with them fails, move the cables back to the source ports on the original device. Click **Revert Destination** to deprovision the destination ports.
11. In the **Task Details** screen, select the iMGs connected to the ports you cut over, then click **Update DHCP Client**.

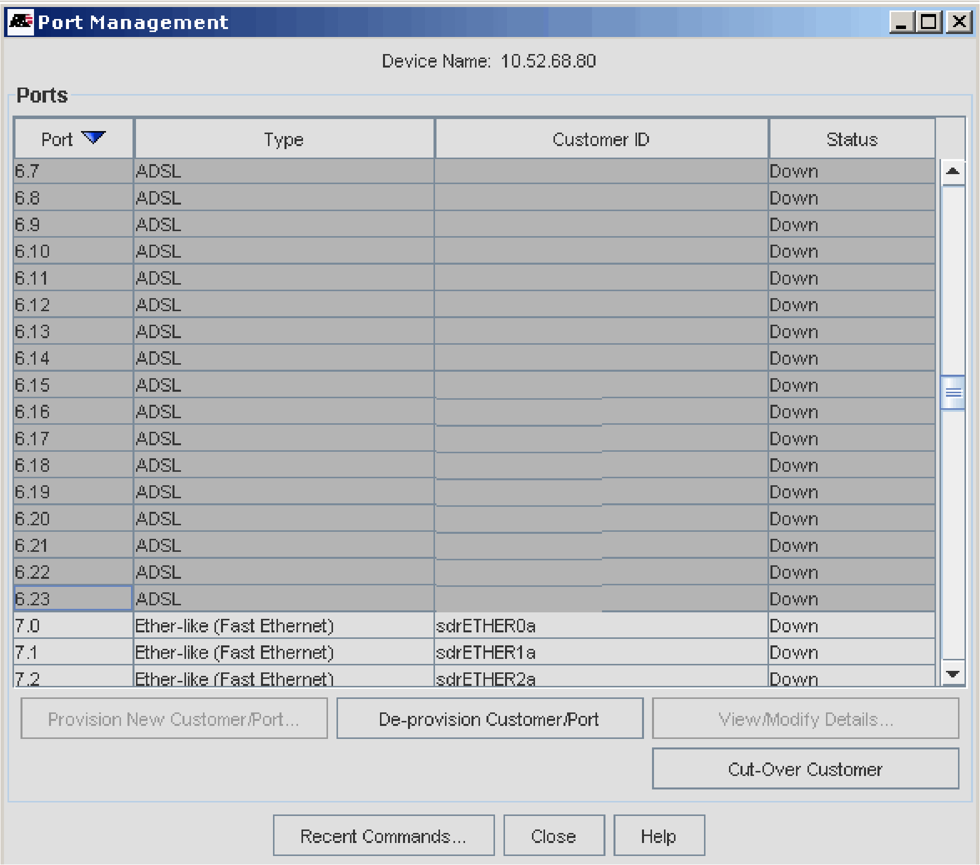
When the iMGs are successfully updated, their status changes to **DHCP Updated**.

Note: An iMG must be powered on and have VLAN IP connectivity before you update the DHCP client.

12. In the **Task Details** screen, select the cut over ports and click **Complete**. The NMS updates the database with the iMG attributes and deprovisions the source ports.

12.7.5.1 Viewing the Source Ports After a Customer Cutover

After performing the customer cutover, you can view the source ports in the **Port Management** screen. The **Customer ID** for all of the source ports is blank and their **Status** is **Down**. At this point you can reprovision the ports for another interface or follow the process to remove the card.



Device Name: 10.52.68.80

Port	Type	Customer ID	Status
6.7	ADSL		Down
6.8	ADSL		Down
6.9	ADSL		Down
6.10	ADSL		Down
6.11	ADSL		Down
6.12	ADSL		Down
6.13	ADSL		Down
6.14	ADSL		Down
6.15	ADSL		Down
6.16	ADSL		Down
6.17	ADSL		Down
6.18	ADSL		Down
6.19	ADSL		Down
6.20	ADSL		Down
6.21	ADSL		Down
6.22	ADSL		Down
6.23	ADSL		Down
7.0	Ether-like (Fast Ethernet)	sdrETHER0a	Down
7.1	Ether-like (Fast Ethernet)	sdrETHER1a	Down
7.2	Ether-like (Fast Ethernet)	sdrETHER2a	Down

FIGURE 12-106 Original Ports Ready to be Reprovisioned

12.7.6 Example: Transferring an iMG to a Different Port

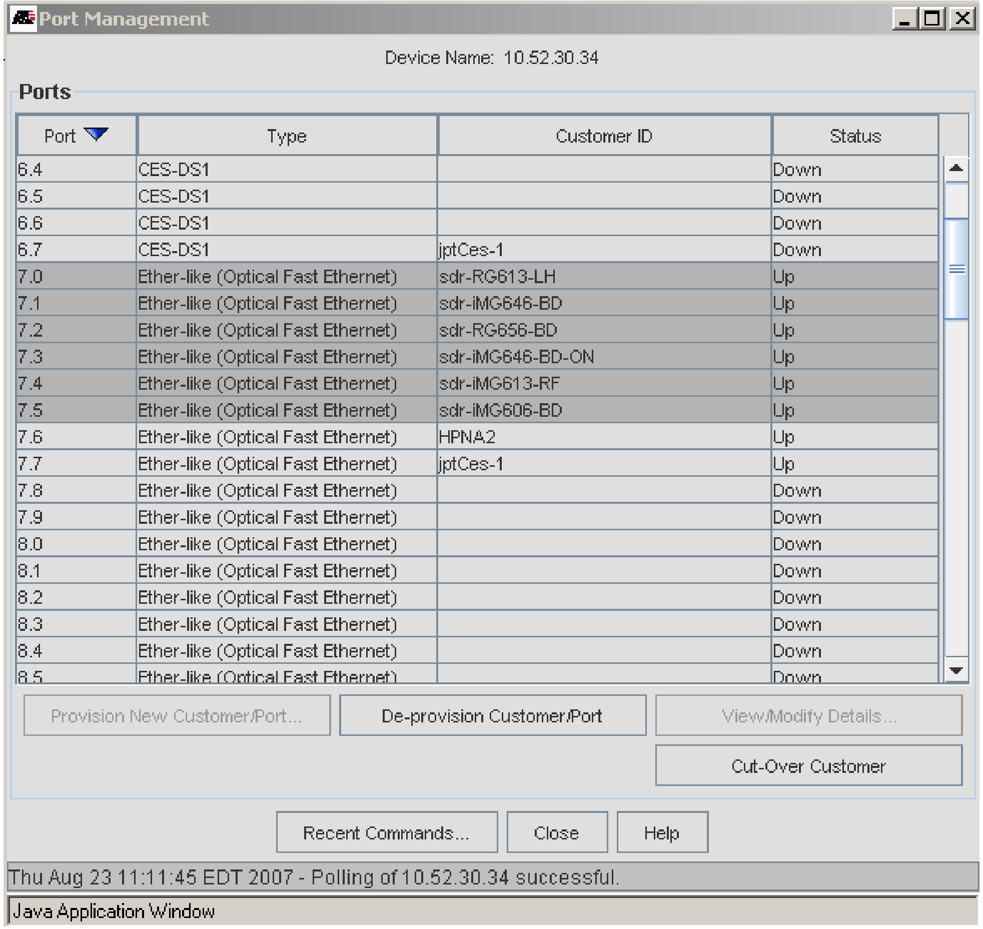
Transferring an iMG from one port to another is a complex operation. In addition to updating the NMS database with the new upstream port, if the iMG's IP address was assigned using DHCP, the iMG must renew its address and update the DHCP-based filters on the iMAP port.

When you are transferring an iMG from one port to another, you can select ADSL, SHDSL, VDSL, or Ether-like ports. In this example, six iMGs are transferred from FX10 to FX20 interfaces. The source and target ports are on the same device. You should perform the provision stage of the cutover process as a separate operation since it may need to be coordinated with the physical hardware cutover, which may need to be performed during off hours.

Caution: If performing cut-over to a different device, the VLAN network must be pre-configured to maintain IP connectivity after the cables are moved over to the new ports. Otherwise, customer cutover to the new port will not complete automatically.

To transfer an iMG from one port to another:

1. Do one of the following in the **Network Objects** panel:
   - Go to **Network Maps** > **Physical Network**. In the **Physical Network** screen, select the device.
   - Go to **Network Inventory** > **Nodes**. In the **Nodes** screen, select the device.
2. Go to **Operations** > **Provision** > **Port Management**. The **Port Management** window appears.



Device Name: 10.52.30.34

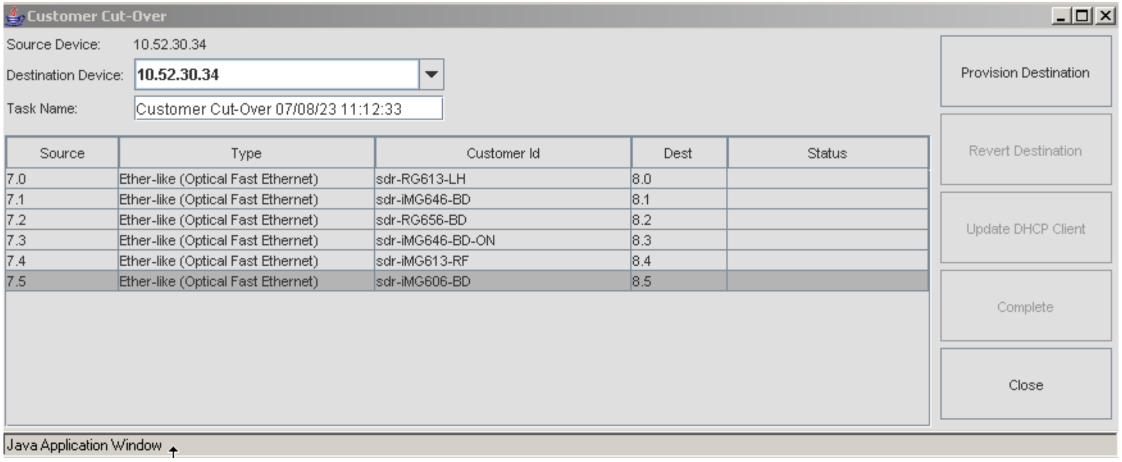
Ports

Port	Type	Customer ID	Status
6.4	CES-DS1		Down
6.5	CES-DS1		Down
6.6	CES-DS1		Down
6.7	CES-DS1	jptCes-1	Down
7.0	Ether-like (Optical Fast Ethernet)	sdr-RG613-LH	Up
7.1	Ether-like (Optical Fast Ethernet)	sdr-iMG646-BD	Up
7.2	Ether-like (Optical Fast Ethernet)	sdr-RG656-BD	Up
7.3	Ether-like (Optical Fast Ethernet)	sdr-iMG646-BD-ON	Up
7.4	Ether-like (Optical Fast Ethernet)	sdr-iMG613-RF	Up
7.5	Ether-like (Optical Fast Ethernet)	sdr-iMG606-BD	Up
7.6	Ether-like (Optical Fast Ethernet)	HPNA2	Up
7.7	Ether-like (Optical Fast Ethernet)	jptCes-1	Up
7.8	Ether-like (Optical Fast Ethernet)		Down
7.9	Ether-like (Optical Fast Ethernet)		Down
8.0	Ether-like (Optical Fast Ethernet)		Down
8.1	Ether-like (Optical Fast Ethernet)		Down
8.2	Ether-like (Optical Fast Ethernet)		Down
8.3	Ether-like (Optical Fast Ethernet)		Down
8.4	Ether-like (Optical Fast Ethernet)		Down
8.5	Ether-like (Optical Fast Ethernet)		Down

Thu Aug 23 11:11:45 EDT 2007 - Polling of 10.52.30.34 successful.

FIGURE 12-107 Selecting Source Ports for iMG Cutover

3. Select the iMGs to cut over.
4. Click **Cut-Over Customer**. The **Customer Cut-Over** screen appears.



Source Device: 10.52.30.34

Destination Device: 10.52.30.34

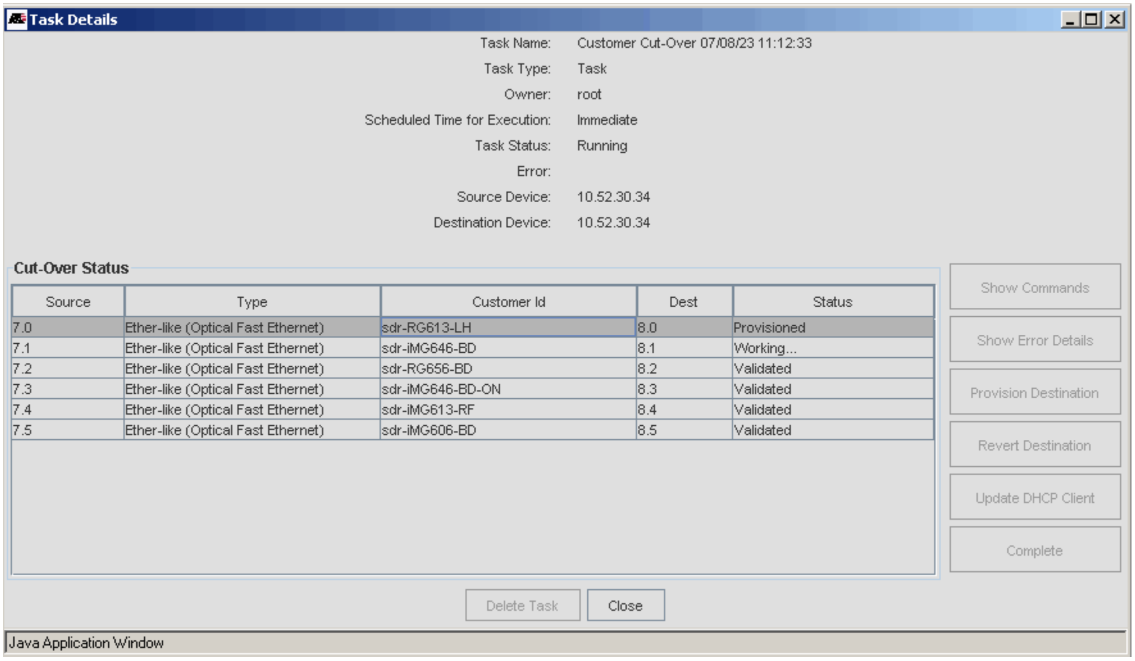
Task Name: Customer Cut-Over 07/08/23 11:12:33

Source	Type	Customer Id	Dest	Status
7.0	Ether-like (Optical Fast Ethernet)	sdr-RG613-LH	8.0	
7.1	Ether-like (Optical Fast Ethernet)	sdr-iMG646-BD	8.1	
7.2	Ether-like (Optical Fast Ethernet)	sdr-RG656-BD	8.2	
7.3	Ether-like (Optical Fast Ethernet)	sdr-iMG646-BD-ON	8.3	
7.4	Ether-like (Optical Fast Ethernet)	sdr-iMG613-RF	8.4	
7.5	Ether-like (Optical Fast Ethernet)	sdr-iMG606-BD	8.5	

FIGURE 12-108 Destination Ports to be Provisioned

5. In the **Destination Device** drop-down list, select the destination device. In this example, the destination device is the same as the source device.
6. If necessary, select the ports in the **Dest** column, and select new ports from the drop-down list.

7. Select all of the rows and click **Provision Destination**. The NMS validates the the source and destination ports and displays the status of the transfer as the task completes.



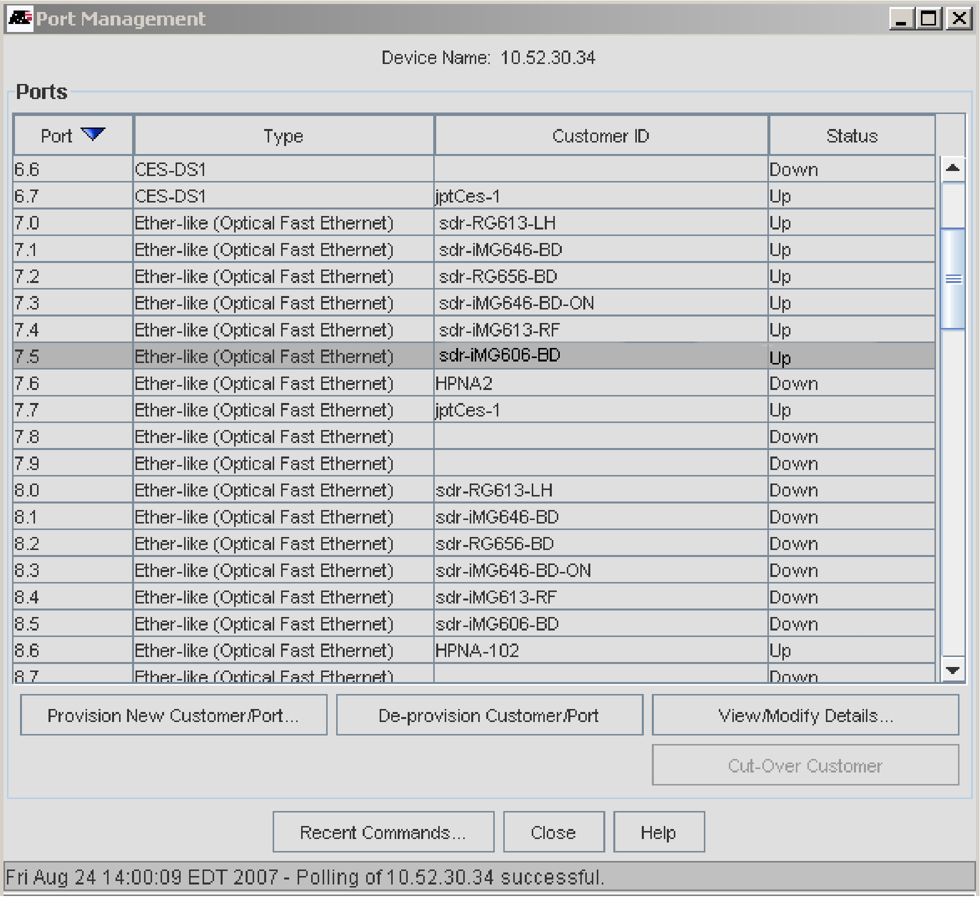
Task Name: Customer Cut-Over 07/08/23 11:12:33
Task Type: Task
Owner: root
Scheduled Time for Execution: Immediate
Task Status: Running
Error:
Source Device: 10.52.30.34
Destination Device: 10.52.30.34

Cut-Over Status

Source	Type	Customer Id	Dest	Status
7.0	Ether-like (Optical Fast Ethernet)	sdr-RG613-LH	8.0	Provisioned
7.1	Ether-like (Optical Fast Ethernet)	sdr-iMG646-BD	8.1	Working...
7.2	Ether-like (Optical Fast Ethernet)	sdr-RG656-BD	8.2	Validated
7.3	Ether-like (Optical Fast Ethernet)	sdr-iMG646-BD-ON	8.3	Validated
7.4	Ether-like (Optical Fast Ethernet)	sdr-iMG613-RF	8.4	Validated
7.5	Ether-like (Optical Fast Ethernet)	sdr-iMG606-BD	8.5	Validated

FIGURE 12-109 Task Details Panel as Target Ports are Provisioned

When the provisioning process is complete, the source ports have a status of **Up**, and the destination ports have the same customer ID as the source ports and have a status of **Down**.



Device Name: 10.52.30.34

Port	Type	Customer ID	Status
6.6	CES-DS1		Down
6.7	CES-DS1	jptCes-1	Up
7.0	Ether-like (Optical Fast Ethernet)	sdr-RG613-LH	Up
7.1	Ether-like (Optical Fast Ethernet)	sdr-iMG646-BD	Up
7.2	Ether-like (Optical Fast Ethernet)	sdr-RG656-BD	Up
7.3	Ether-like (Optical Fast Ethernet)	sdr-iMG646-BD-ON	Up
7.4	Ether-like (Optical Fast Ethernet)	sdr-iMG613-RF	Up
7.5	Ether-like (Optical Fast Ethernet)	sdr-iMG606-BD	Up
7.6	Ether-like (Optical Fast Ethernet)	HPNA2	Down
7.7	Ether-like (Optical Fast Ethernet)	jptCes-1	Up
7.8	Ether-like (Optical Fast Ethernet)		Down
7.9	Ether-like (Optical Fast Ethernet)		Down
8.0	Ether-like (Optical Fast Ethernet)	sdr-RG613-LH	Down
8.1	Ether-like (Optical Fast Ethernet)	sdr-iMG646-BD	Down
8.2	Ether-like (Optical Fast Ethernet)	sdr-RG656-BD	Down
8.3	Ether-like (Optical Fast Ethernet)	sdr-iMG646-BD-ON	Down
8.4	Ether-like (Optical Fast Ethernet)	sdr-iMG613-RF	Down
8.5	Ether-like (Optical Fast Ethernet)	sdr-iMG606-BD	Down
8.6	Ether-like (Optical Fast Ethernet)	HPNA-102	Up
8.7	Ether-like (Optical Fast Ethernet)		Down

Fri Aug 24 14:00:09 EDT 2007 - Polling of 10.52.30.34 successful.

FIGURE 12-110 Port Attributes Transferred to Destination Ports

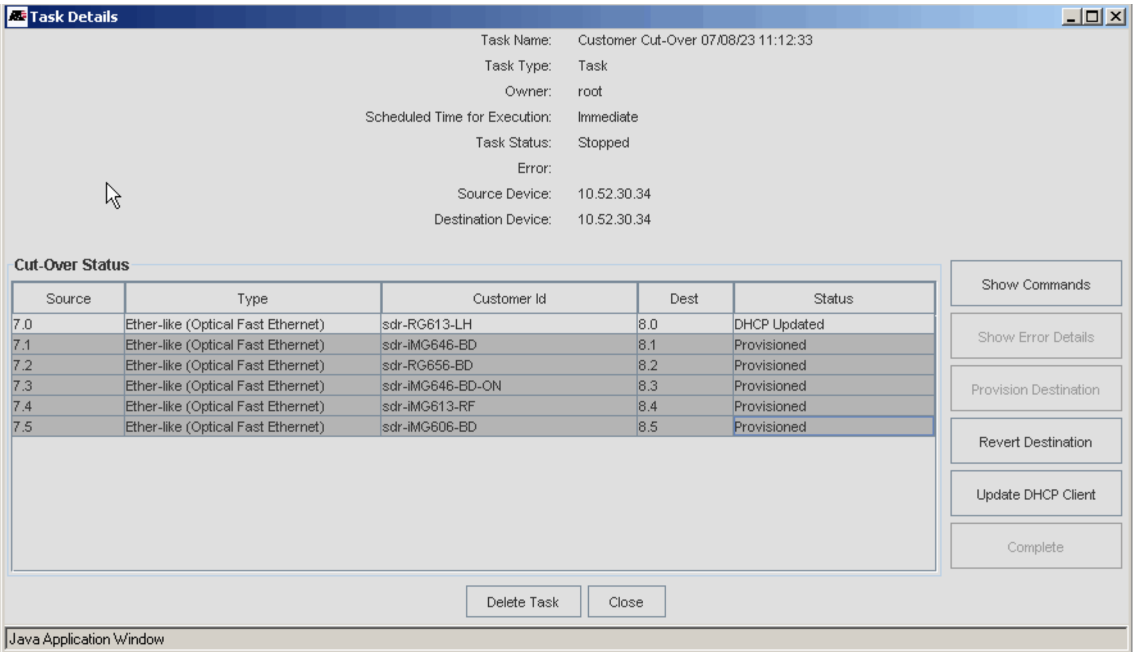
8. Disconnect the optic fiber from the FX10 interfaces and connect them to the FX20 interfaces.

Note: *You may need to change cabling facilities to connect FX10 cables to the FX20 interfaces. Refer to the iMAP Component Specification for information on FX10 and FX20 cabling types.*

The port is now active and is physically connected to the iMG, but the iMG must renew its IP address (if assigned using DHCP) to update DHCP-based filtering on the iMAP port.

9. In the **Task Details** screen, select the iMGs connected to the ports you cut over, then click **Update DHCP Client**. When the **iMGs** are updated, the status changes to **DHCP Updated**.

Note: *The iMGs must be powered on and have VLAN IP connectivity before you update the DHCP client.*

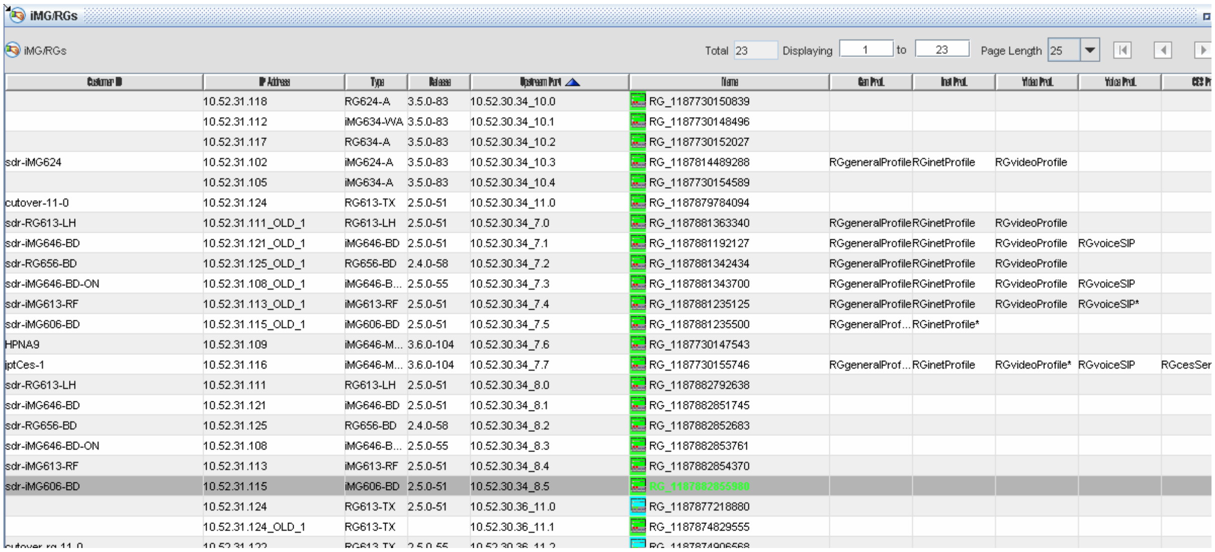


Task Name: Customer Cut-Over 07/08/23 11:12:33
Task Type: Task
Owner: root
Scheduled Time for Execution: Immediate
Task Status: Stopped
Error:
Source Device: 10.52.30.34
Destination Device: 10.52.30.34

Cut-Over Status

Source	Type	Customer Id	Dest	Status
7.0	Ether-like (Optical Fast Ethernet)	sdr-RG613-LH	8.0	DHCP Updated
7.1	Ether-like (Optical Fast Ethernet)	sdr-iMG646-BD	8.1	Provisioned
7.2	Ether-like (Optical Fast Ethernet)	sdr-RG656-BD	8.2	Provisioned
7.3	Ether-like (Optical Fast Ethernet)	sdr-iMG646-BD-ON	8.3	Provisioned
7.4	Ether-like (Optical Fast Ethernet)	sdr-iMG613-RF	8.4	Provisioned
7.5	Ether-like (Optical Fast Ethernet)	sdr-iMG606-BD	8.5	Provisioned

FIGURE 12-111 Selecting iMGs and Updating the DHCP Client

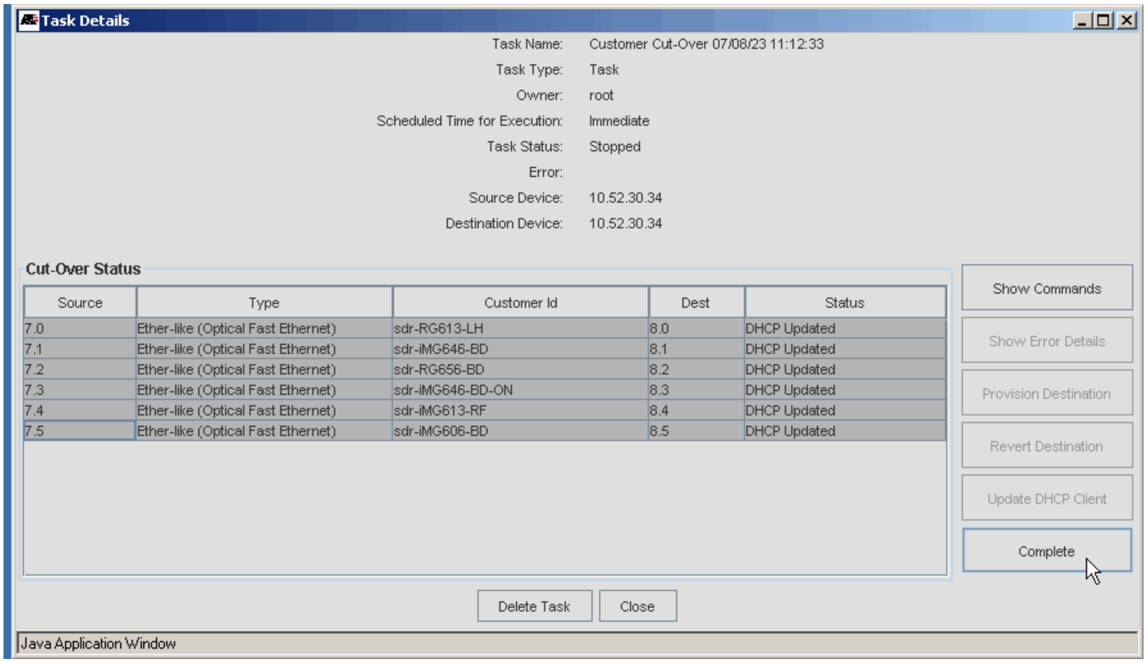


Total 23 Displaying 1 to 23 Page Length 25

Customer ID	IP Address	Type	Release	Upstream Port	Name	Gen Prof.	Inet Prof.	Video Prof.	Voice Prof.	CES Pr
	10.52.31.118	RG624-A	3.5.0-83	10.52.30.34_10.0	RG_1187730150839					
	10.52.31.112	iMG634-WA	3.5.0-83	10.52.30.34_10.1	RG_1187730148496					
	10.52.31.117	RG634-A	3.5.0-83	10.52.30.34_10.2	RG_1187730152027					
sdr-iMG624	10.52.31.102	iMG624-A	3.5.0-83	10.52.30.34_10.3	RG_1187814489288	RGgeneralProfile	RGinetProfile	RGvideoProfile		
	10.52.31.105	iMG634-A	3.5.0-83	10.52.30.34_10.4	RG_1187730154589					
cutover-11-0	10.52.31.124	RG613-TX	2.5.0-51	10.52.30.34_11.0	RG_1187879784094					
sdr-RG613-LH	10.52.31.111_OLD_1	RG613-LH	2.5.0-51	10.52.30.34_7.0	RG_1187881363340	RGgeneralProfile	RGinetProfile	RGvideoProfile		
sdr-iMG646-BD	10.52.31.121_OLD_1	iMG646-BD	2.5.0-51	10.52.30.34_7.1	RG_1187881192127	RGgeneralProfile	RGinetProfile	RGvideoProfile	RGvoiceSIP	
sdr-RG656-BD	10.52.31.125_OLD_1	RG656-BD	2.4.0-58	10.52.30.34_7.2	RG_1187881342434	RGgeneralProfile	RGinetProfile	RGvideoProfile		
sdr-iMG646-BD-ON	10.52.31.108_OLD_1	iMG646-B...	2.5.0-55	10.52.30.34_7.3	RG_1187881343700	RGgeneralProfile	RGinetProfile	RGvideoProfile	RGvoiceSIP	
sdr-iMG613-RF	10.52.31.113_OLD_1	iMG613-RF	2.5.0-51	10.52.30.34_7.4	RG_1187881235125	RGgeneralProfile	RGinetProfile	RGvideoProfile	RGvoiceSIP*	
sdr-iMG606-BD	10.52.31.115_OLD_1	iMG606-BD	2.5.0-51	10.52.30.34_7.5	RG_1187881235500	RGgeneralProf...	RGinetProfile*			
HPNA9	10.52.31.109	iMG646-M...	3.6.0-104	10.52.30.34_7.6	RG_1187730147543					
iptCes-1	10.52.31.116	iMG646-M...	3.6.0-104	10.52.30.34_7.7	RG_1187730155746	RGgeneralProf...	RGinetProfile	RGvideoProfile*	RGvoiceSIP	RGcesSer
sdr-RG613-LH	10.52.31.111	RG613-LH	2.5.0-51	10.52.30.34_8.0	RG_1187882792638					
sdr-iMG646-BD	10.52.31.121	iMG646-BD	2.5.0-51	10.52.30.34_8.1	RG_1187882851745					
sdr-RG656-BD	10.52.31.125	RG656-BD	2.4.0-58	10.52.30.34_8.2	RG_1187882852683					
sdr-iMG646-BD-ON	10.52.31.108	iMG646-B...	2.5.0-55	10.52.30.34_8.3	RG_1187882853761					
sdr-iMG613-RF	10.52.31.113	iMG613-RF	2.5.0-51	10.52.30.34_8.4	RG_1187882854370					
sdr-iMG606-BD	10.52.31.115	iMG606-BD	2.5.0-51	10.52.30.34_8.5	RG_1187882855980					
	10.52.31.124	RG613-TX	2.5.0-51	10.52.30.36_11.0	RG_1187877218880					
	10.52.31.124_OLD_1	RG613-TX		10.52.30.36_11.1	RG_1187874829555					
cutover-rg-11-0	10.52.31.122	RG613-TX	2.5.0-55	10.52.30.36_11.2	RG_1187874906568					

FIGURE 12-112 DHCP Recovery Complete

10. In the **Task Details** screen, select the cut over ports and click **Complete**. The NMS updates the database with the iMG attributes and deprovisions the source ports.



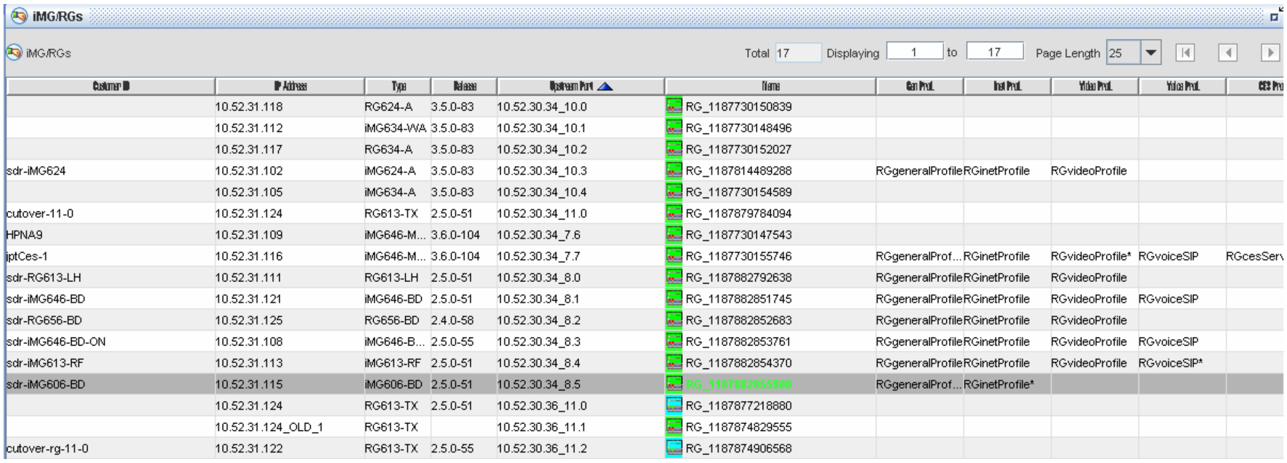
Task Name: Customer Cut-Over 07/08/23 11:12:33
Task Type: Task
Owner: root
Scheduled Time for Execution: Immediate
Task Status: Stopped
Error:
Source Device: 10.52.30.34
Destination Device: 10.52.30.34

Cut-Over Status

Source	Type	Customer Id	Dest	Status
7.0	Ether-like (Optical Fast Ethernet)	sdr-RG613-LH	8.0	DHCP Updated
7.1	Ether-like (Optical Fast Ethernet)	sdr-iMG646-BD	8.1	DHCP Updated
7.2	Ether-like (Optical Fast Ethernet)	sdr-RG656-BD	8.2	DHCP Updated
7.3	Ether-like (Optical Fast Ethernet)	sdr-iMG646-BD-ON	8.3	DHCP Updated
7.4	Ether-like (Optical Fast Ethernet)	sdr-iMG613-RF	8.4	DHCP Updated
7.5	Ether-like (Optical Fast Ethernet)	sdr-iMG606-BD	8.5	DHCP Updated

FIGURE 12-113 Completing the iMG Cutover

When the provisioning is complete, the iMG table shows the new upstream ports.



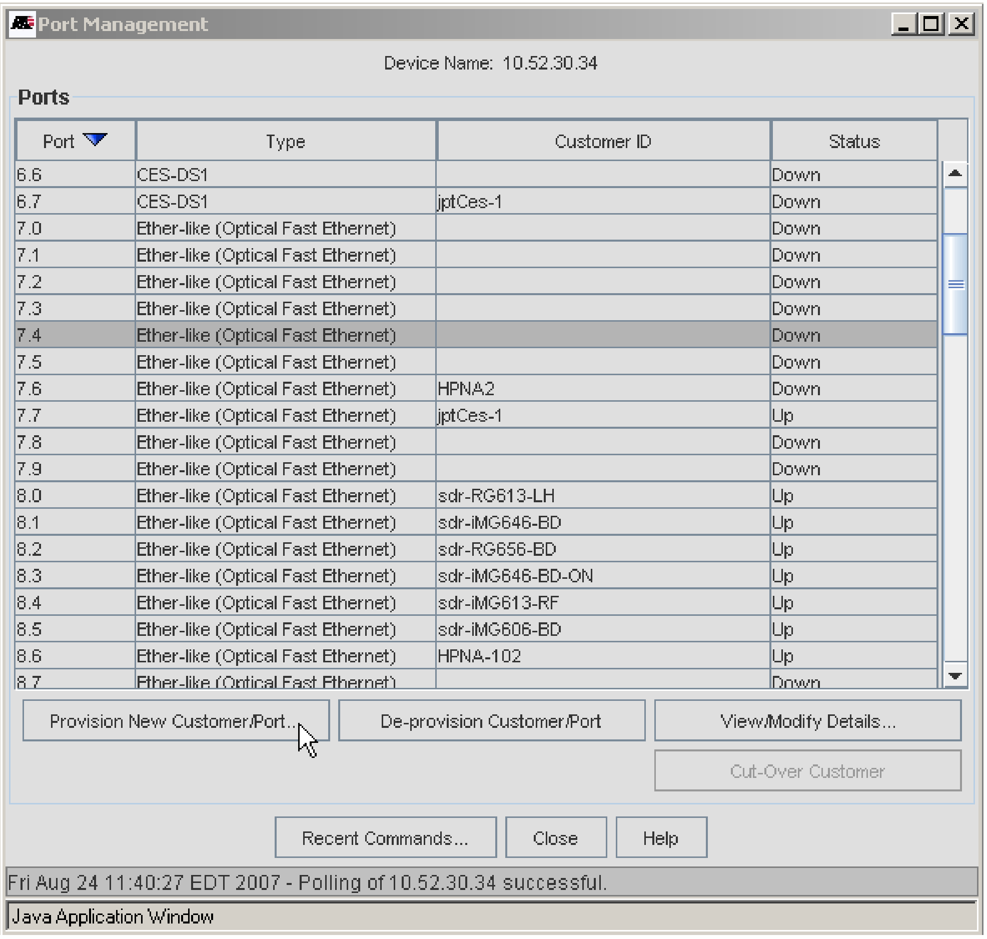
Total 17 Displaying 1 to 17 Page Length 25

Customer ID	IP Address	Type	Release	Upstream Port	Name	Gen Prof.	Inet Prof.	Video Prof.	Voice Prof.	CES Pro
	10.52.31.118	RG624-A	3.5.0-83	10.52.30.34_10.0	RG_1187730150839					
	10.52.31.112	iMG634-WA	3.5.0-83	10.52.30.34_10.1	RG_1187730148496					
	10.52.31.117	RG634-A	3.5.0-83	10.52.30.34_10.2	RG_1187730152027					
sdr-iMG624	10.52.31.102	iMG624-A	3.5.0-83	10.52.30.34_10.3	RG_1187814489288	RGgeneralProfile	RGinetProfile	RGvideoProfile		
	10.52.31.105	iMG634-A	3.5.0-83	10.52.30.34_10.4	RG_1187730154589					
cutover-11-0	10.52.31.124	RG613-TX	2.5.0-51	10.52.30.34_11.0	RG_1187879784094					
HPNA9	10.52.31.109	iMG646-M...	3.6.0-104	10.52.30.34_7.6	RG_1187730147543					
iptCes-1	10.52.31.116	iMG646-M...	3.6.0-104	10.52.30.34_7.7	RG_1187730155746	RGgeneralProf...	RGinetProfile	RGvideoProfile*	RGvoiceSIP	RGcesServ
sdr-RG613-LH	10.52.31.111	RG613-LH	2.5.0-51	10.52.30.34_8.0	RG_1187882792638	RGgeneralProfile	RGinetProfile	RGvideoProfile		
sdr-iMG646-BD	10.52.31.121	iMG646-BD	2.5.0-51	10.52.30.34_8.1	RG_1187882851745	RGgeneralProfile	RGinetProfile	RGvideoProfile	RGvoiceSIP	
sdr-RG656-BD	10.52.31.125	RG656-BD	2.4.0-58	10.52.30.34_8.2	RG_1187882852683	RGgeneralProfile	RGinetProfile	RGvideoProfile		
sdr-iMG646-BD-ON	10.52.31.108	iMG646-B...	2.5.0-55	10.52.30.34_8.3	RG_1187882853761	RGgeneralProfile	RGinetProfile	RGvideoProfile	RGvoiceSIP	
sdr-iMG613-RF	10.52.31.113	iMG613-RF	2.5.0-51	10.52.30.34_8.4	RG_1187882854370	RGgeneralProfile	RGinetProfile	RGvideoProfile	RGvoiceSIP*	
sdr-iMG606-BD	10.52.31.115	iMG606-BD	2.5.0-51	10.52.30.34_8.5	RG_1187882855980	RGgeneralProf...	RGinetProfile*			
	10.52.31.124	RG613-TX	2.5.0-51	10.52.30.36_11.0	RG_1187877218880					
	10.52.31.124_OLD_1	RG613-TX		10.52.30.36_11.1	RG_1187874829555					
cutover-rg-11-0	10.52.31.122	RG613-TX	2.5.0-55	10.52.30.36_11.2	RG_1187874906568					

FIGURE 12-114 iMG/RG Table when Provisioning is Complete

12.7.6.1 Viewing the Source Ports After a Customer Cutover

After performing the customer cutover, you can view the source ports in the **Port Management** screen. The **Customer ID** for all of the source ports is blank and their **Status** is **Down**. At this point you can reprovision the ports for another interface or follow the process to remove the card.



Device Name: 10.52.30.34

Ports

Port	Type	Customer ID	Status
6.6	CES-DS1		Down
6.7	CES-DS1	jptCes-1	Down
7.0	Ether-like (Optical Fast Ethernet)		Down
7.1	Ether-like (Optical Fast Ethernet)		Down
7.2	Ether-like (Optical Fast Ethernet)		Down
7.3	Ether-like (Optical Fast Ethernet)		Down
7.4	Ether-like (Optical Fast Ethernet)		Down
7.5	Ether-like (Optical Fast Ethernet)		Down
7.6	Ether-like (Optical Fast Ethernet)	HPNA2	Down
7.7	Ether-like (Optical Fast Ethernet)	jptCes-1	Up
7.8	Ether-like (Optical Fast Ethernet)		Down
7.9	Ether-like (Optical Fast Ethernet)		Down
8.0	Ether-like (Optical Fast Ethernet)	sdr-RG613-LH	Up
8.1	Ether-like (Optical Fast Ethernet)	sdr-iMG646-BD	Up
8.2	Ether-like (Optical Fast Ethernet)	sdr-RG656-BD	Up
8.3	Ether-like (Optical Fast Ethernet)	sdr-iMG646-BD-ON	Up
8.4	Ether-like (Optical Fast Ethernet)	sdr-iMG613-RF	Up
8.5	Ether-like (Optical Fast Ethernet)	sdr-iMG606-BD	Up
8.6	Ether-like (Optical Fast Ethernet)	HPNA-102	Up
8.7	Ether-like (Optical Fast Ethernet)		Down

Fri Aug 24 11:40:27 EDT 2007 - Polling of 10.52.30.34 successful.

Java Application Window

FIGURE 12-115 Original Ports Ready to be Reprovisioned

13. Card Management

Card Management is for iMAP and SBx3100 devices. You can view all cards in a device and configure each card. The Card Management table updates in real-time as changes occur.

You can perform the following tasks with Card Management:

- Using Card Management
- Creating a Card
- Enabling a Card
- Disabling a Card
- Restarting a Card
- Destroying a Card
- Downloading Card Software
- Viewing Recent Commands
- Viewing Card Details

13.1 Supported Cards

The following cards support Card Management.

13.1.1 iMAP Cards

Service modules:

- FE10
- FX10FX
- FX10LX
- FX10BX
- FX20BX
- FX20BX40
- ADSL24B
- ADSL24A
- ADSL24AE
- ADSL24SA
- ADSL48A
- ADSL48B
- POTS24
- POTS24C
- PAC24A

- PAC24AH
- PAC24C
- SHDSL24
- CES8
- GE8
- GE24BX
- EPON2
- VDSL24A
- VDSL24B

Network modules:

- GE3
- GE4
- NTE8
- GE2RJ
- GE8
- XE1
- XE1S
- XE6

Control modules:

- CFC100
- CFC100GX
- CFC56
- CFC24
- CFC12

13.1.2 SBx3100 cards

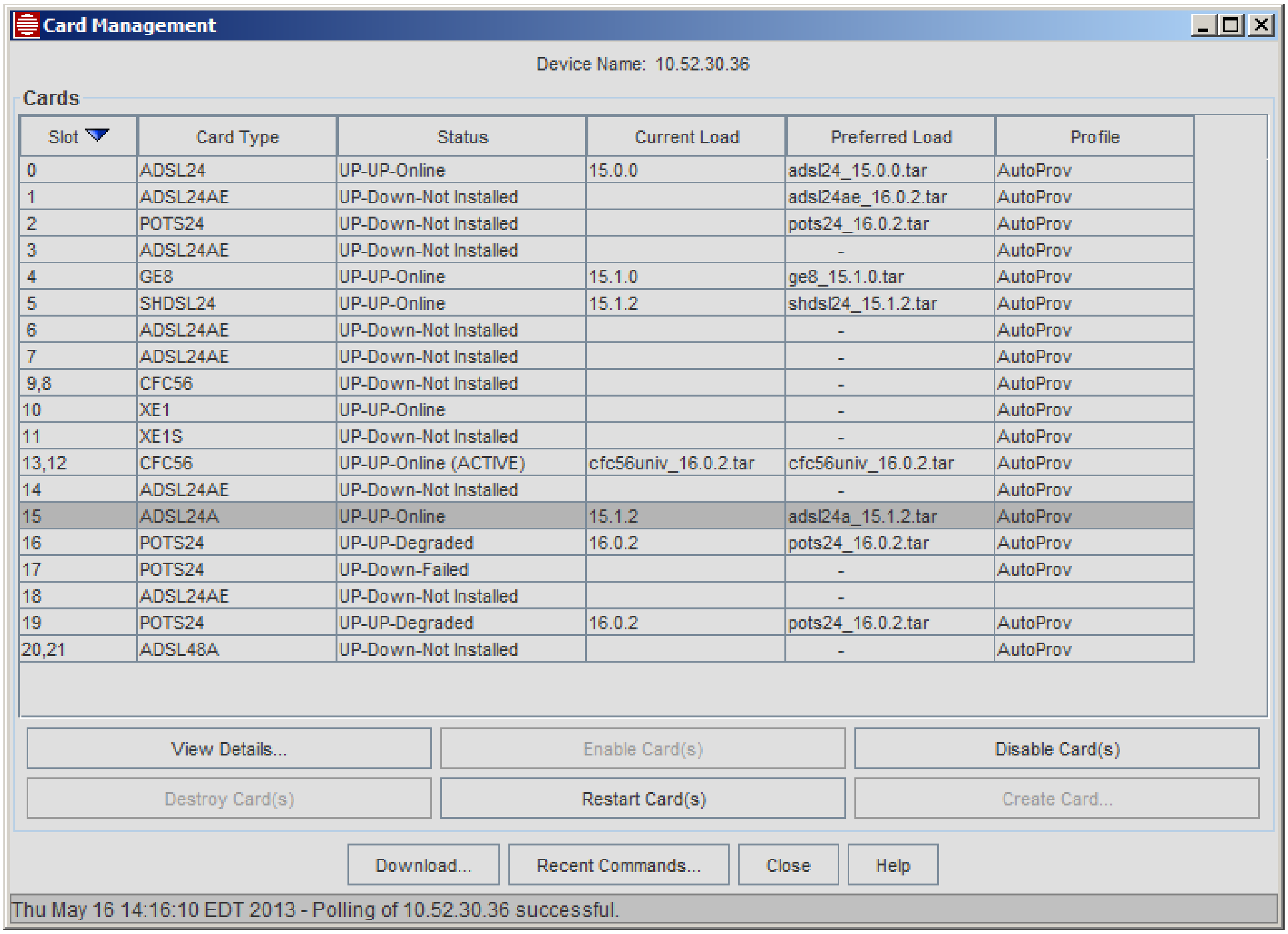
- CFC200
- CFC960
- GE40CSFP
- GE40RJ
- GE24POE
- GE24RJ
- GE24SFP
- XE6SFP
- XE4

13.2 Using Card Management

1. Do one of the following in the **Network Objects** panel:
    - Go to **Network Maps** > **Physical Network**. In the **Physical Network** screen, select the device.

- Go to **Network Inventory** > **Nodes**. In the **Nodes** screen, select the device.

2. Go to **Operations** > **Provision** > **Card Management**. The **Card Management** window appears.



Device Name: 10.52.30.36

Slot	Card Type	Status	Current Load	Preferred Load	Profile
0	ADSL24	UP-UP-Online	15.0.0	adsl24_15.0.0.tar	AutoProv
1	ADSL24AE	UP-Down-Not Installed		adsl24ae_16.0.2.tar	AutoProv
2	POTS24	UP-Down-Not Installed		pots24_16.0.2.tar	AutoProv
3	ADSL24AE	UP-Down-Not Installed		-	AutoProv
4	GE8	UP-UP-Online	15.1.0	ge8_15.1.0.tar	AutoProv
5	SHDSL24	UP-UP-Online	15.1.2	shdsl24_15.1.2.tar	AutoProv
6	ADSL24AE	UP-Down-Not Installed		-	AutoProv
7	ADSL24AE	UP-Down-Not Installed		-	AutoProv
9,8	CFC56	UP-Down-Not Installed		-	AutoProv
10	XE1	UP-UP-Online		-	AutoProv
11	XE1S	UP-Down-Not Installed		-	AutoProv
13,12	CFC56	UP-UP-Online (ACTIVE)	cfc56univ_16.0.2.tar	cfc56univ_16.0.2.tar	AutoProv
14	ADSL24AE	UP-Down-Not Installed		-	AutoProv
15	ADSL24A	UP-UP-Online	15.1.2	adsl24a_15.1.2.tar	AutoProv
16	POTS24	UP-UP-Degraded	16.0.2	pots24_16.0.2.tar	AutoProv
17	POTS24	UP-Down-Failed		-	AutoProv
18	ADSL24AE	UP-Down-Not Installed		-	
19	POTS24	UP-UP-Degraded	16.0.2	pots24_16.0.2.tar	AutoProv
20,21	ADSL48A	UP-Down-Not Installed		-	AutoProv

Thu May 16 14:16:10 EDT 2013 - Polling of 10.52.30.36 successful.

FIGURE 13-1 Card Management

Card Management contains the following fields:

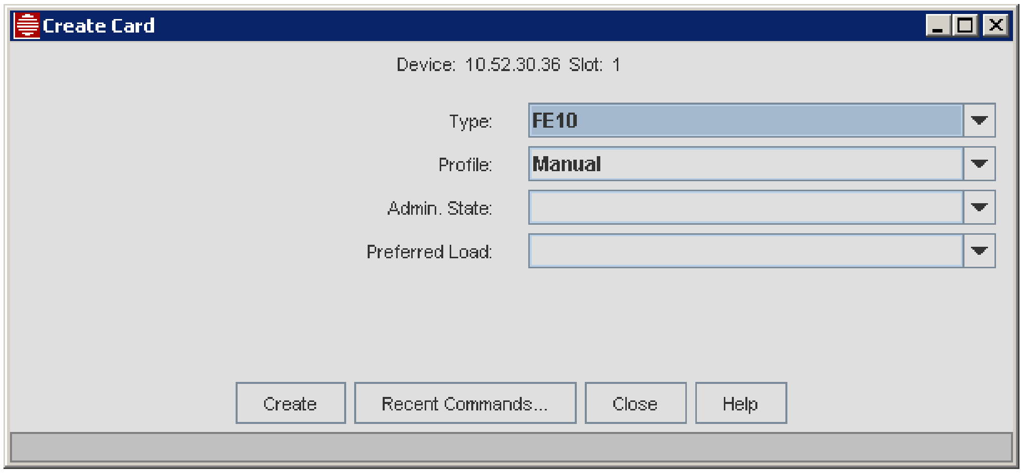
Field	Description
Device Name	The name of the device.
Slot	The slot in the device that contains the card.
Card Type	The type of card. See Supported Cards.

Field	Description
Status	The current status of the card displayed as <Administrative State>-<Operational State>-<Status> Administrative State - Reflects whether the card is UP (available for service) or Down. You control the Administrative State by enabling or disabling the card. Operational State - UP (providing service) or Down. The Operational State is dependent on the Administrative State as follows: • If the Administrative State of a card is UP, the Operational State will be UP if the card/port can provide service. • If the Administrative State is Down, the Operational State will always be Down. Status - The current status of the card as Online, Offline, Not Installed, Degraded or Failed.
Current Load	The load currently in the card’s flash memory.
Preferred Load	The primary load that the card will use when it restarts.
Profile	Shows whether the card is in Auto-Provisioning or Manually Provisioned mode. See Overview of Provisioning Data, Profiles, and Card States for a description of provisioning modes.
View Details	Displays the current attributes of the type card. Refer to Overview of Provisioning Data, Profiles, and Card States.
Download	Views the files currently on the FLASH memory of the cards and allows files to be deleted or downloaded. The available load can then be downloaded using the Download button. This button is also available on the Card Details window. Refer to Controlling Card Software (Download and Restart).

13.3 Creating a Card

You can create provisioning data for a card before or after the card is physically present in the device.

1. Do one of the following in the **Network Objects** panel:
   - Go to **Network Maps** > **Physical Network**. In the **Physical Network** screen, select the device.
   - Go to **Network Inventory** > **Nodes**. In the **Nodes** screen, select the device.
2. Go to **Operations** > **Provision** > **Card Management**. The **Card Management** window appears.
3. Select a row that does not have a card type defined.
4. Click **Create Card**. The **Create Card** window appears.



Create Card

Device: 10.52.30.36 Slot: 1

Type: FE10

Profile: Manual

Admin. State:

Preferred Load:

FIGURE 13-2 Create Card

5. In the **Type** drop-down list, select the type of card you want to provision. The types of cards available will depend on the device.
6. In the **Profile** drop-down list, select **Manual** or **AutoProv**. If you select **AutoProv** for a card that is not installed yet the card will automatically provision when you insert it in the slot.

Note: When you select AutoProv for the Profile the rest of the fields in the Create Card window are grayed out.

7. If you selected **Manual** for the **Profile**, in the **Admin State** drop-down list, select Up or Down for the Administrative State.
   - Up - The card is automatically enabled and will attempt to go into service. When the card is in service its Operational State will change to UP.
   - Down - The card is created and disabled.
8. If you selected **Manual** for the **Profile**, in the **Preferred Load** drop-down list, select the software load that will load when the card restarts. In most cases the preferred load should be the same as the current running load. This option is only available for cards that utilize a software load.
9. The following cards have additional settings:
   - CES8 and NTE8 - In the **Ports Type** drop-down list, select **DS1** or **E1** as the port type.
   - POTS24 - In the **POTS Protocol** drop-down list, select **MGCP** or **SIP** as the POTS protocol.
   - SHDSL24 - In the **Annex Type** drop-down list, select **A** or **B**.
10. Click **Create** to create the card. The **Card Management** window is updated with the new card.

13.4 Enabling a Card

1. Do one of the following in the **Network Objects** panel:
   - Go to **Network Maps** > **Physical Network**. In the **Physical Network** screen, select the device.
   - Go to **Network Inventory** > **Nodes**. In the **Nodes** screen, select the device.
2. Go to **Operations** > **Provision** > **Card Management**. The **Card Management** window appears.
3. Select one or more cards you want to enable. A card must be disabled in order to enable it. In the Status field, a disabled card will have an Administrative State of Down.
4. Click **Enable Card(s)**. The selected cards are enabled and the Administrative State for each changes to UP.

13.5 Disabling a Card

1. Do one of the following in the **Network Objects** panel:
   - Go to **Network Maps** > **Physical Network**. In the **Physical Network** screen, select the device.
   - Go to **Network Inventory** > **Nodes**. In the **Nodes** screen, select the device.
2. Go to **Operations** > **Provision** > **Card Management**. The **Card Management** window appears.
3. Select one or more cards you want to disable. A card must be enabled in order to disable it. In the Status field, an enabled card will have an Administrative State of UP.
4. Click **Disable Card(s)**, then click **Yes** to confirm the action. The selected cards are disabled and the Administrative State for each changes to Down.

13.6 Restarting a Card

1. Do one of the following in the **Network Objects** panel:
   - Go to **Network Maps** > **Physical Network**. In the **Physical Network** screen, select the device.
   - Go to **Network Inventory** > **Nodes**. In the **Nodes** screen, select the device.
2. Go to **Operations** > **Provision** > **Card Management**. The **Card Management** window appears.

3. Select one or more cards you want to restart. The cards must be provisioned and physically present to restart.
4. Click **Restart Card(s)**, then click **Yes** to confirm the action and restart the cards.

13.7 Destroying a Card

Before you can destroy a card you must disable it. Destroying a card removes its provisioning from the database and leaves the slot empty in the **Card Management** window.

1. Do one of the following in the **Network Objects** panel:
   - Go to **Network Maps** > **Physical Network**. In the **Physical Network** screen, select the device.
   - Go to **Network Inventory** > **Nodes**. In the **Nodes** screen, select the device.
2. Go to **Operations** > **Provision** > **Card Management**. The **Card Management** window appears.
3. Select one or more cards you want to destroy. Before you can destroy a card you must disable it. In the Status field, a disabled card will have an Administrative State of Down.
4. Click **Destroy Card(s)**, then click **Yes** to confirm the action. The selected cards are destroyed and the **Card Management** window is updated to reflect empty slots.

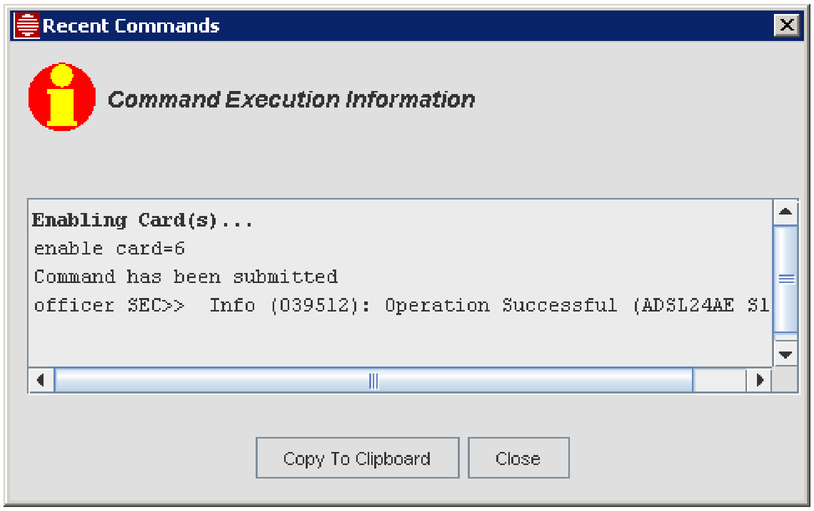
13.8 Downloading Card Software

Views the files currently on the FLASH memory of the cards and allows files to be deleted or downloaded. The available load can then be downloaded using the Download button. This button is also available on the Card Details window. Refer to Controlling Card Software (Download and Restart).

13.9 Viewing Recent Commands

You can review a listing of the CLI commands and responses for the most recent Card Management operation.

1. After performing a Card Management operation, click **Recent Commands**. The Recent Commands window appears.



```
Enabling Card(s)...
enable card=6
Command has been submitted
officer SEC>>  Info (039512): Operation Successful (ADSL24AE S1
```

FIGURE 13-3 Recent Commands

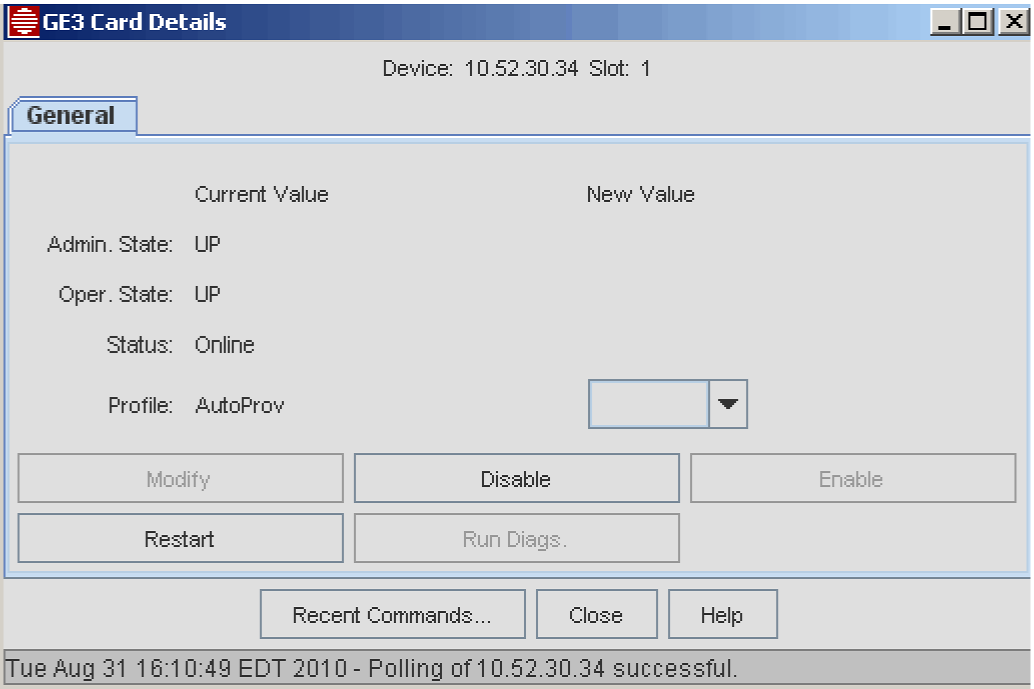
2. Click **Copy To Clipboard** to copy the contents to the clipboard. You can paste the text into any text editor.
3. Click **Close** to close the **Recent Commands** window.

13.10 Viewing Card Details

1. Do one of the following in the **Network Objects** panel:
   - Go to **Network Maps** > **Physical Network**. In the **Physical Network** screen, select the device.
   - Go to **Network Inventory** > **Nodes**. In the **Nodes** screen, select the device.
2. Go to **Operations** > **Provision** > **Card Management**. The **Card Management** window appears.
3. Select the card you want to view.
4. Click **View Details**. The **Card Details** window appears. The fields in the **Card Details** window vary depending on the card you selected.

13.11 GE3 Card

After selecting a GE3, the user can select *View Details*, which provides specific information on the card and includes some of the same options available on the Card Management table. Refer to Figure 13-4 and Table 13-1.



Device: 10.52.30.34 Slot: 1

Admin. State: UP

Oper. State: UP

Status: Online

Profile: AutoProv

Tue Aug 31 16:10:49 EDT 2010 - Polling of 10.52.30.34 successful.

FIGURE 13-4 GE3 Card Details

TABLE 13-1 GE3 Card Details

Field/Button	Description
Device	The device name and the slot number for the card (0 or 1 for the iMAP 9400, 10 or 11 for the iMAP 7700.
Admin. State	If UP, the GE3 is capable of providing service. If DOWN, can Run Diags.
Oper. State	The GE3 is providing service. This state is not controllable but depends on the Admin. State.
Status	The current state of the card. States can be static or dynamic (transition of state such as Initializing or Running Tests).
Profile	The template for provisioning data. The default is AutoProv. If the blank pull-down is chosen, there is no profile (manually provisioned).

TABLE 13-1 GE3 Card Details

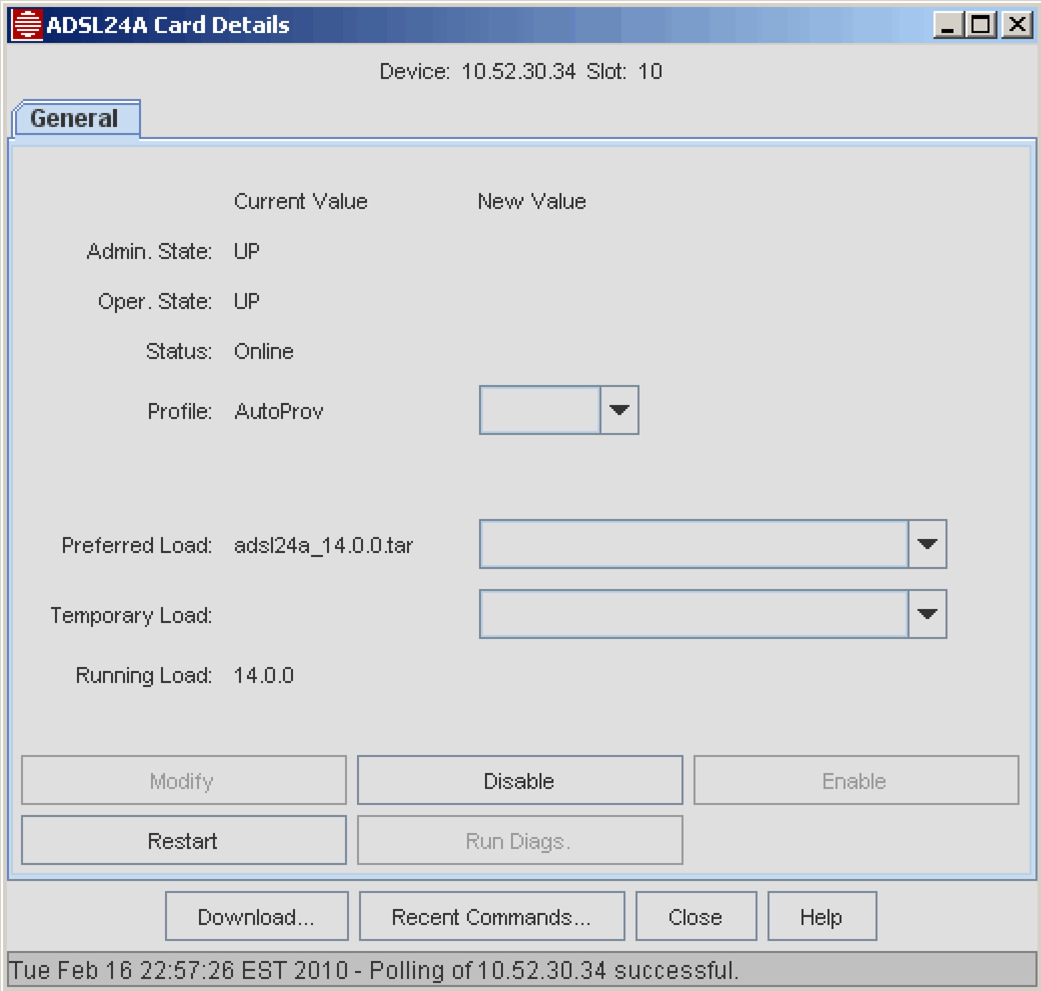
Field/Button	Description
Modify	Activated when the Profile is changed.
Disable	Disables the card. Active only when the Admin State is UP.
Enable	Enables the card. Active only when the Admin State is DOWN.
Restart	Reboots the card. For the GE1, there is no software load.
Run Diags	Runs diagnostics. Active only when the Admin state is DOWN, so must Disable first.

13.12 GE8 Card

The attributes and options are the same as for the GE3 card except that the GE8 has a software load, described in GE3 Card.

13.13 ADSL24A Card

After selecting an ADSL24A card, the user can select *View Details*, providing specific information on the card and some of the same options available on the Card Management table. Refer to Figure 13-5 and Table 13-2.


ADSL24A Card Details

Device: 10.52.30.34 Slot: 10

General

	Current Value	New Value
Admin. State:	UP	
Oper. State:	UP	
Status:	Online	
Profile:	AutoProv	
Preferred Load:	adsl24a_14.0.0.tar	
Temporary Load:		
Running Load:	14.0.0	

Tue Feb 16 22:57:26 EST 2010 - Polling of 10.52.30.34 successful.

FIGURE 13-5 ADSL24A Card Details

TABLE 13-2 ADSL Card Details

Field/Button	Description
Device	The device name and the slot number for the card (5-11 for the iMAP MAP 9400, 0-7, 14-21 for the iMAP MAP 9700 in duplex mode.
Admin. State	If UP, the ADSL is capable of providing service. If DOWN, can Run Diags.
Oper. State	The ADSL is providing service. This state is not controllable but depends on the Admin. State.
Status	The current state of the card. States can be static or dynamic (transition of state such as Initializing or Running Tests).
Profile	The template for provisioning data. The default is AutoProv. If the blank pull-down is chosen, there is no profile (manually provisioned).
Preferred Load	This is the software that will load when the card restarts. In normal operation this should be the same as the running load. This is used during software upgrades.
Temporary Load	This is software that will load the next time the card restarts, and is part of the software upgrade process.
Running Load	The software that is currently on the FLASH of the card.
Modify	Activated when the Profile, Preferred Load, or Temporary Load is changed, is changed.
Disable	Disables the card. Active only when the Admin State is UP.
Enable	Enables the card. Active only when the Admin State is DOWN.
Restart	Reboots the card. The load used will be the Running Load unless the preferred or temporary load has been specified, such as during an upgrade.
Run Diags	Runs diagnostics. Active only when the Admin state is DOWN, so must Disable first.
Download‘	Brings up the Download Software window. Refer to Controlling Card Software (Download and Restart).

13.14 ADSL24 (Annex B) and ADSL24AE

The ADSL24 Annex B and ADSL24AE cards have the same attributes as the ADSL24A card. Refer to ADSL24A Card.

Note: *The NMS cannot distinguish annex A from annex B for ADSL24 cards Users need to know which annex their cards are. When selecting a preferred load or a temporary load, the annex a file is adsl24_*.tar and the annex b file is adsl24xb_*.tar.*

13.15 SHDSL24 Card (Card-Level vs. Port-Level)

SHDSL (Symmetric Highspeed Digital Subscriber Line) is an international standard for symmetric DSL that provides for sending and receiving high-speed symmetrical data streams over a single or dual pair of copper wires and supports Annex-B service for data and voice.

There are the standard card fields as well as Annex Type. Bonding mode controlled on a port basis.

13.16 CFC Cards

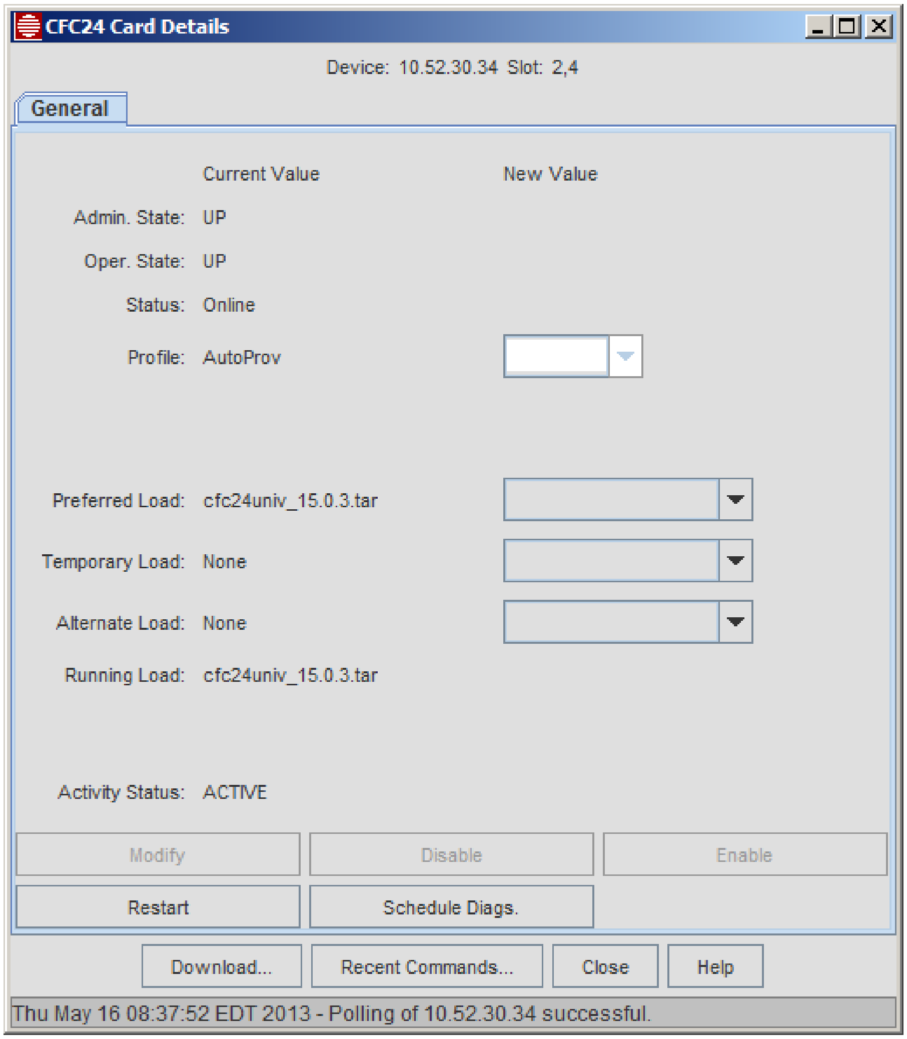
The NMS supports the following CFC cards:

- CFC24
- CFC56
- CFC100
- CFC100GX

- CFC200

CFC cards can be in either simplex or duplex mode. To view a CFC card in simplex mode:

1. In the **Physical Network** screen, select the device.
2. Go to **Operations** > **Provision** > **Card Management** to bring up the **Card Management** form.
3. Select the card you want to view and click **View Details**. The **Card Details** window appears.



CFC24 Card Details

Device: 10.52.30.34 Slot: 2,4

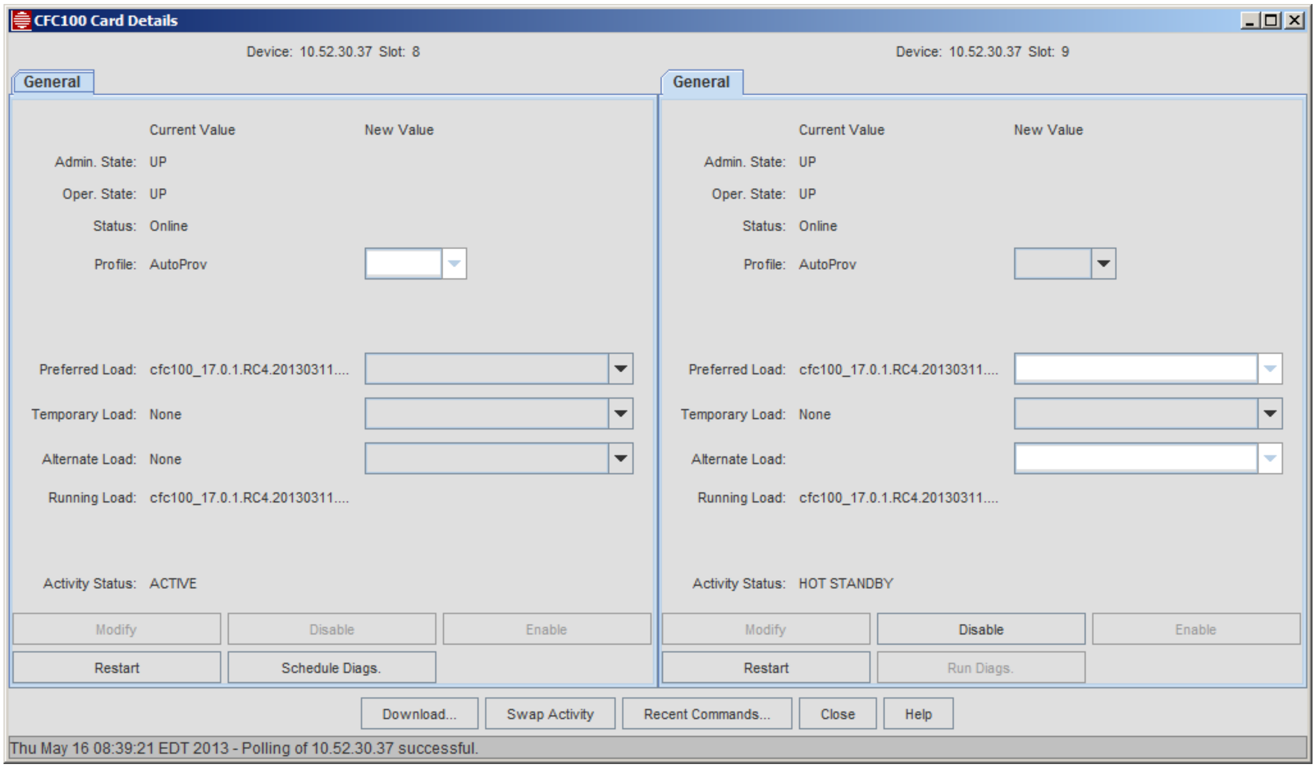
General

	Current Value	New Value
Admin. State:	UP	
Oper. State:	UP	
Status:	Online	
Profile:	AutoProv	
Preferred Load:	cfc24univ_15.0.3.tar	
Temporary Load:	None	
Alternate Load:	None	
Running Load:	cfc24univ_15.0.3.tar	
Activity Status:	ACTIVE	

Thu May 16 08:37:52 EDT 2013 - Polling of 10.52.30.34 successful.

FIGURE 13-6 CFC Card Details (Simplex)

When you view a CFC card in simplex mode, only one CFC is displayed. When you view a CFC in duplex mode, the **Card Details** window includes both CFCs.



CFC100 Card Details

Device: 10.52.30.37 Slot: 8

General

	Current Value	New Value
Admin. State:	UP	
Oper. State:	UP	
Status:	Online	
Profile:	AutoProv	
Preferred Load:	cfc100_17.0.1.RC4.20130311....	
Temporary Load:	None	
Alternate Load:	None	
Running Load:	cfc100_17.0.1.RC4.20130311....	
Activity Status:	ACTIVE	

Device: 10.52.30.37 Slot: 9

General

	Current Value	New Value
Admin. State:	UP	
Oper. State:	UP	
Status:	Online	
Profile:	AutoProv	
Preferred Load:	cfc100_17.0.1.RC4.20130311....	
Temporary Load:	None	
Alternate Load:		
Running Load:	cfc100_17.0.1.RC4.20130311....	
Activity Status:	HOT STANDBY	

Thu May 16 08:39:21 EDT 2013 - Polling of 10.52.30.37 successful.

FIGURE 13-7 CFC Card Details (Duplex)

Table 13-3 lists the information and options available for CFCs in the **Card Details** window. Items specific to duplex mode CFCs are highlighted.

TABLE 13-3 CFC Card Details

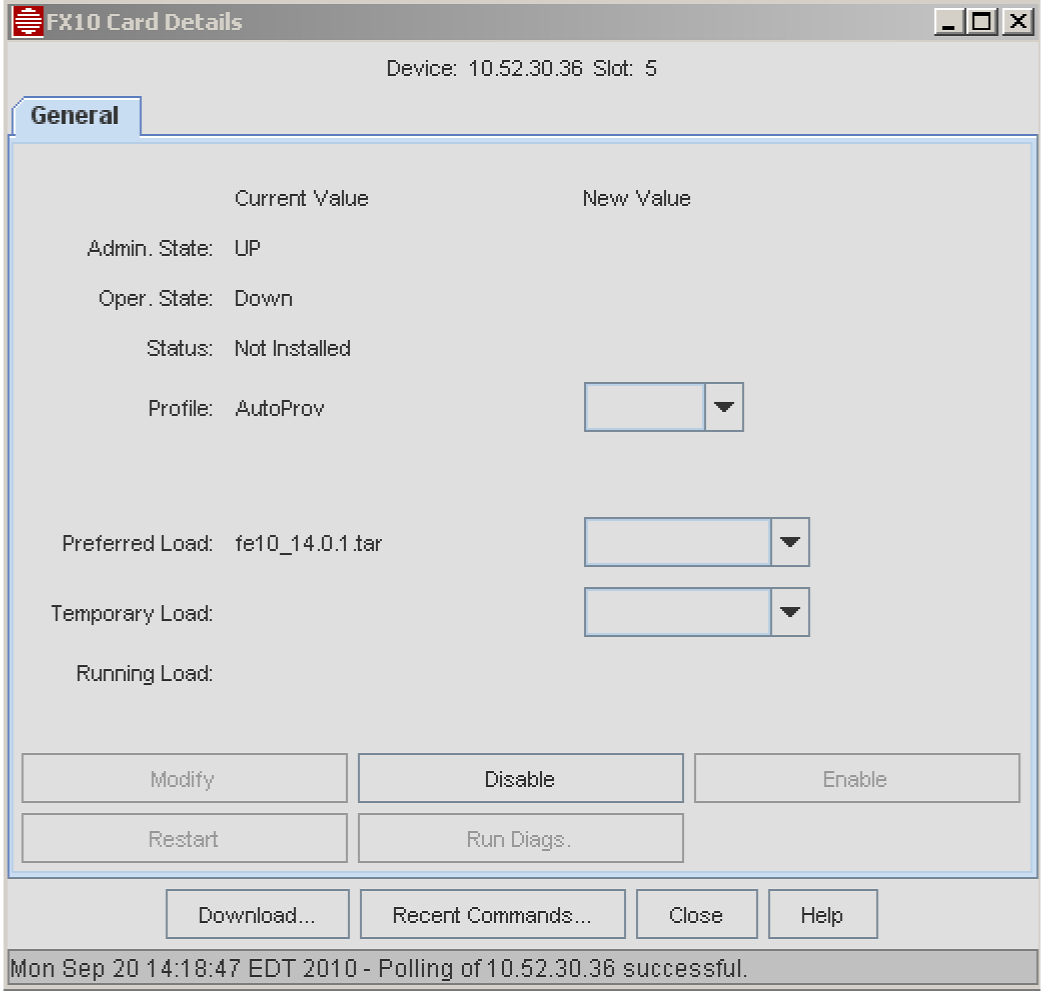
Field/Button	Description
Device	The device name and the slot number for the card.
Admin. State	If UP, the CFC is capable of providing service. In duplex mode both CFCs should be UP. If DOWN, can Schedule Diags.
Oper. State	The CFC is providing service. The operational state depends on the Admin. State. In duplex mode both CFCs should be UP.
Status	The current state of the card. States can be static or dynamic (transition of state such as Initializing or Running Tests). In normal operation CFC cards should be ONLINE for both simplex and duplex.
Profile	The profile used to provision the card. The only selection is manual, since when a profile for a card type is set to AutoProv, the card will automatically provision itself when inserted in that slot.
Preferred Load	This is the software that will load when the card restarts. In normal operation this should be the same as the running load and includes the software that will download to the other cards. This load will be different during software upgrades.
Temporary Load	Software that will load the next time the card restarts. This is part of the software upgrade process.
Alternate Load	An alternate load file.
Running Load	The software that is currently in the card's flash memory. For duplex CFCs in normal operation, the loads should be the same.

TABLE 13-3 CFC Card Details (Continued)

Field/Button	Description
Diags. Result	The status and results of diagnostics set by using the Schedule Diags. button. For an iMAP in simplex mode, these are run with the card in service.
Diags Schedule	States whether the Schedule Diags. button has been used to schedule diagnostics on the active (simplex) or inactive (duplex) CFC card.
Modify	Activated when the Profile, Preferred Load, or Temporary Load is changed.
Disable	Disables the card. Available only when the Admin State is UP. In duplex mode, you cannot disable the ACTIVE CFC.
Enable	Enables the card. Available only when the Admin State is DOWN.
Restart	Reboots the card. The load used will be the Running Load unless the preferred or temporary load has been specified, such as during an upgrade.
Schedule Diags.	Schedules diagnostics. Active only when the Admin state is DOWN, so must Disable first.
Download	Brings up the Download Software window. Refer to Controlling Card Software (Download and Restart).
Swap Activity	Available on the ACTIVE CFC only. Swaps activity from one CFC to the other. For a description of what is involved when you swap CFC activity, see the *Software Reference for iMAP Series Switches*.

13.17 FE10/FX10 Card

Figure 13-8 and Table 13-4 lists the fields/buttons available for the FE10 card.



Device: 10.52.30.36 Slot: 5

	Current Value	New Value
Admin. State:	UP	
Oper. State:	Down	
Status:	Not Installed	
Profile:	AutoProv	
Preferred Load:	fe10_14.0.1.tar	
Temporary Load:		
Running Load:		

Mon Sep 20 14:18:47 EDT 2010 - Polling of 10.52.30.36 successful.

FIGURE 13-8 FE10/FX10 Card Details

TABLE 13-4 FE10/FX10 Card Details

Field/Button	Description
Device	The device name and the slot number for the card.
Admin. State	If UP, the FE10 is capable of providing service. If DOWN, can Run Diags.
Oper. State	The FE10 is providing service. This state is not controllable but depends on the Admin. State.
Status	The current state of the card. States can be static or dynamic (transition of state such as Initializing or Running Tests).
Profile	The template for provisioning data. The default is AutoProv. If the blank pull-down is chosen, there is no profile (manually provisioned).
Preferred Load	This is the software that will load when the card restarts. In normal operation this should be the same as the running load. This is used during software upgrades.
Temporary Load	This is software that will load the next time the card restarts, and is part of the software upgrade process.
Running Load	The software that is currently on the FLASH of the card.

TABLE 13-4 FE10/FX10 Card Details

Field/Button	Description
Modify	Activated when the Profile is changed.
Disable	Disables the card. Active only when the Admin State is UP.
Enable	Enables the card. Active only when the Admin State is DOWN.
Restart	Reboots the card. For the FE10, there is no software load.
Run Diags	Runs diagnostics. Active only when the Admin state is DOWN, so must Disable first.

13.18 FX20 Card

The FX10/FX20 Card Details form is similar to the FE10, shown in Figure 13-8.

13.19 POTS24 Card

The iMAP POTS24/POTS24C card (referred to forward as POTS24) is a single slot service module that provides 24 analog loopstart line circuits on the iMAP system.The POTS24 card supports VoIP using:

- MGCP (Media Gateway Control Protocol)
- Session Initiated Protocol (SIP)

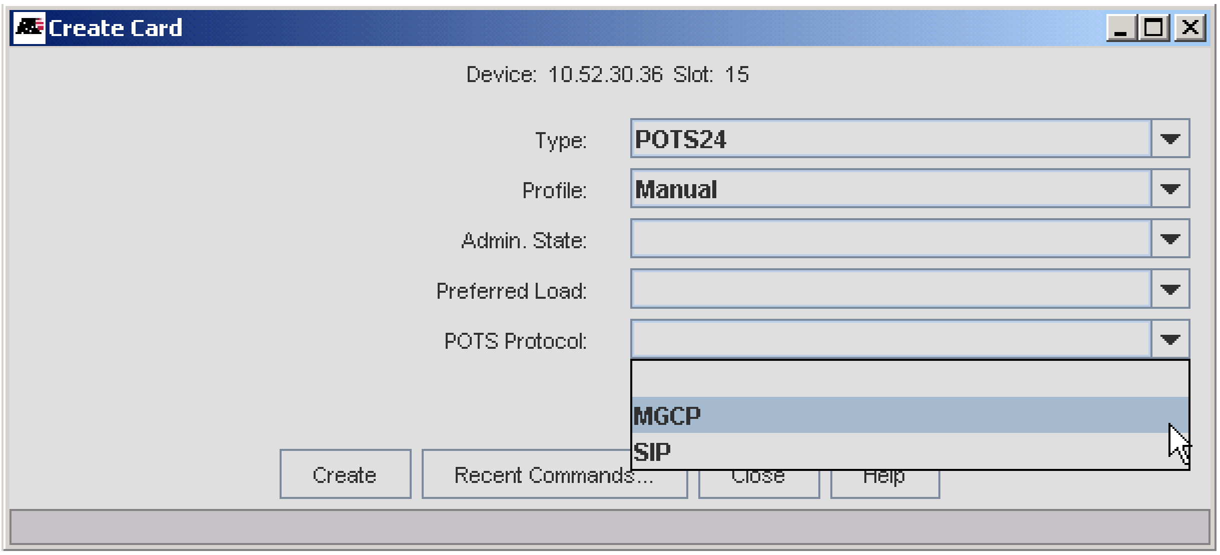
The RTP (Real-Time Protocol, RFC 3550) configuration specifies how the card will exchange bearer packets with the call agent over the network. Once the IP provisioning is done for the card's virtual Ethernet interface, the RTP attributes can be provisioned.

Note: *The POTS24 must have IP, MGCP/SIP, and RTP protocol attributes provisioned in association with the card in order to provide service. Therefore, the POTS24 card cannot be completely auto-provisioned to an in-service state; some manual configuration is required for each card that cannot be specified in the auto-provisioning profiles. For a full explanation of these attributes, refer to the section on provisioning POTS in the Software Reference for iMAP Series Switches.*

Note: *Any modification of RTP parameters requires the card to be disabled*

Note: *There are separate software loads for the POTS24 card, one for supporting MGCP and another for supporting SIP. Therefore, one card can only support one type of protocol or the other.*

Figure 13-10 shows the POTS24 Card Create Form which shows the protocol choice, while subsequent figures show the POTS24 Card Details Form and how they display MGCP or SIP attributes. Note that the IP/RTP subtab of the Protocols tab has the same values regardless of whether MGCP or SIP is configured.

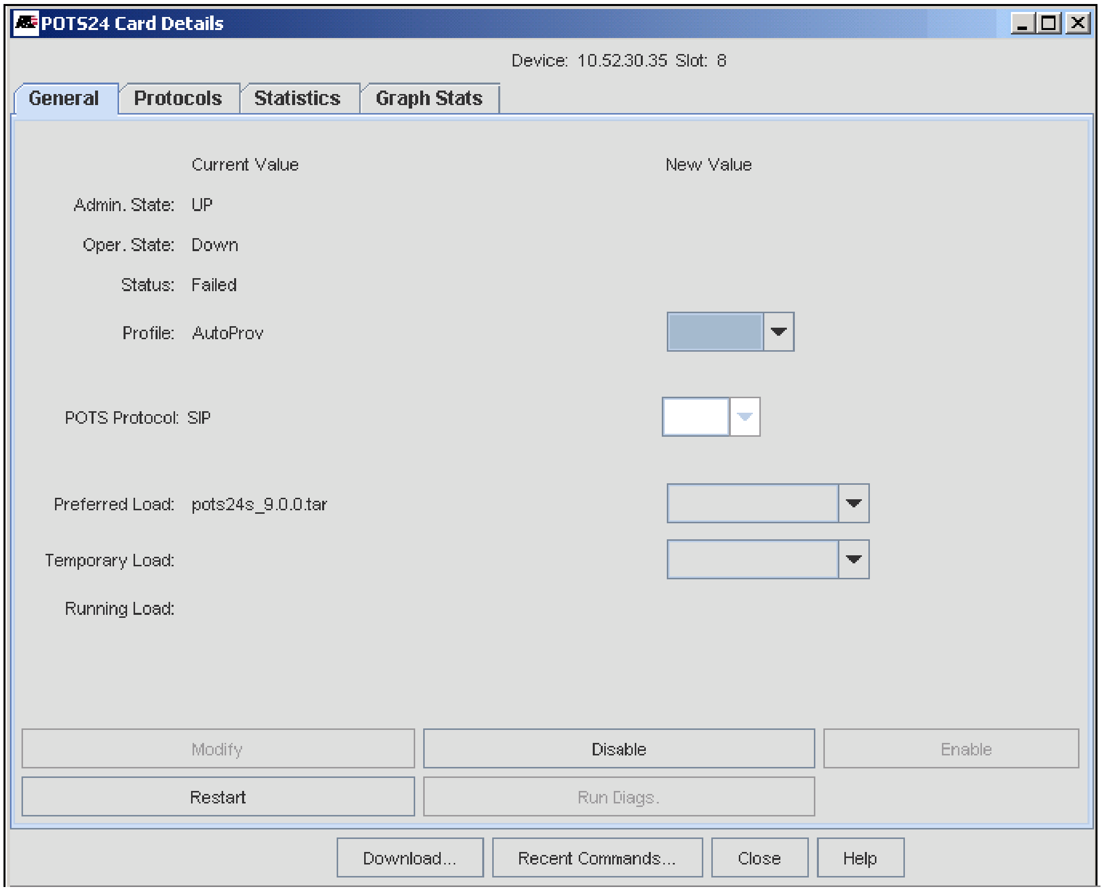


Create Card

Device: 10.52.30.36 Slot: 15

Type:	POTS24
Profile:	Manual
Admin. State:	
Preferred Load:	
POTS Protocol:	

FIGURE 13-9 Create POTS 24 Card Form



POTS24 Card Details

Device: 10.52.30.35 Slot: 8

	Current Value	New Value
Admin. State:	UP	
Oper. State:	Down	
Status:	Failed	
Profile:	AutoProv	
POTS Protocol:	SIP	
Preferred Load:	pots24s_9.0.0.tar	
Temporary Load:		
Running Load:		

FIGURE 13-10 Card Management - POTS24 - General Tab

13.19.1 POTS24 Card - General Tab

TABLE 13-5 POTS24 Card Details - General Tab

Field/Button	Description
Device	The device name and the slot number for the card.
Admin. State	If UP, the POTS24 is capable of providing service. If DOWN, can Run Diags.
Oper. State	The POTS24 is providing service. This state is not controllable but depends on the Admin. State.
Status	The current state of the card. States can be static or dynamic (transition of state such as Initializing or Running Tests).
Profile	The template for provisioning data. *Note: The profile is Manually Provisioned. Refer to the above Note.*
POTS Protocol	Whether the card is using MGCP or SIP. *Note: If the card is enabled, this pull-down is not available.*
Preferred Load	This is the software that will load when the card restarts. In normal operation this should be the same as the running load, and includes the software that will download to the POTS24 card. This load will be different during software upgrades. *Note: Loads that support SIP have the label POTS24S (versus POTS24).*
Temporary Load	This is software that will load the next time the card restarts, and is part of the software upgrade process, so this is usually empty.
Running Load	An alternate load file.
Modify	Activated when the Profile is changed.
Disable	Disables the card. Active only when the Admin State is UP.
Enable	Enables the card. Active only when the Admin State is DOWN.
Restart	Reboots the card. If there is a Temporary Load, this will be loaded onto the card.
Run Diags	Runs diagnostics. Active only when the Admin state is DOWN, so must Disable first.
Download	Brings up the Download Software window. Refer to Controlling Card Software (Download and Restart).

13.19.2 POTS24 Card - Protocols/IP/RTP Tab

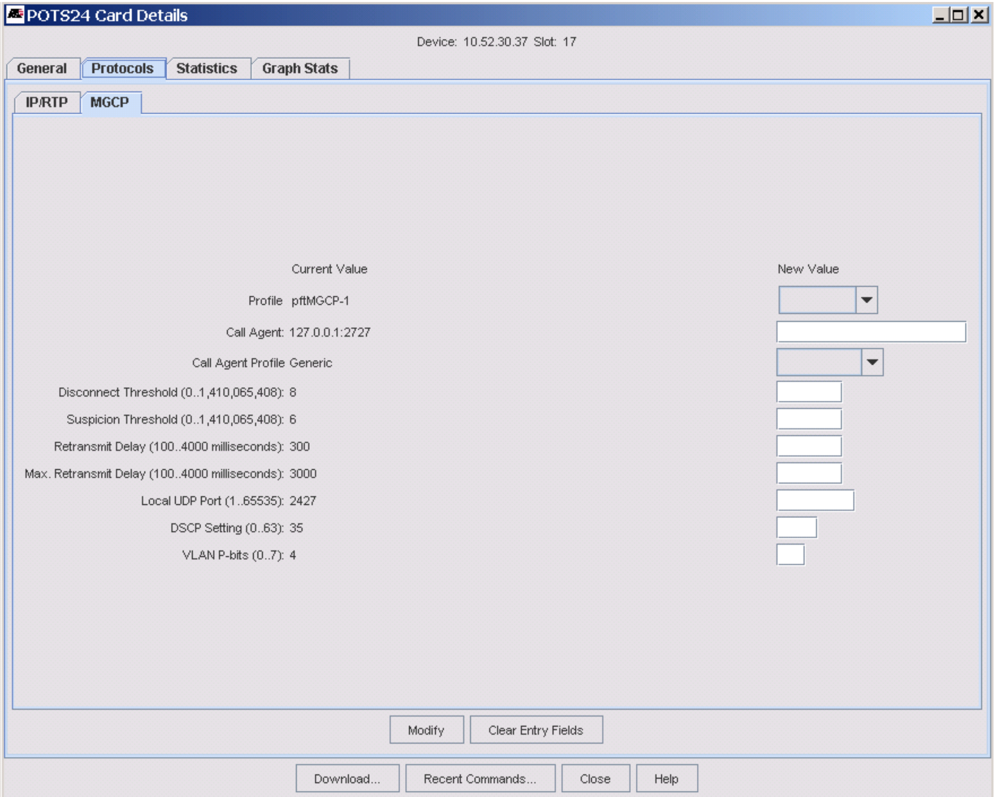
TABLE 13-6 POTS24 Card Details - Protocols Tab for IP/RTP

Field/Button	Description
IP	
VLAN vid (2..4094):	Specification of the interface in terms of VLAN id. A logical representation of a port. An id must be a VID number
IP Address	IP address of the interface.
Subnet Mask	Subnet mask of the interface.
Gateway	Optional gateway address for the interface.
DNS Server	Domain name server (DNS) for the card. Use only when the MGCP Call Agent is a DNS host name.
Domain Name	Optional domain name for the interface.

TABLE 13-6 POTS24 Card Details - Protocols Tab for IP/RTP

Field/Button	Description
RTP	
DSCP Settings	The DSCP (Differentiated Services Code Point, RFC 2474) value for RTP packets transmitted from the POTS24 card. The default value is **46**.
VLAN P bits (0..7)	The 802.1p priority bit setting for RTP packets transmitted from the POTS24 card. The default value is **6**.
Modify	Activated when a value has been changed. WHen selected, makes the changes to the card.
Clear Entry Fields	Clears all changed values
Download	Brings up the Download Software window. Refer to Controlling Card Software (Download and Restart).

13.19.3 POTS24 Card - Protocols - MGCP Tab



Device: 10.52.30.37 Slot: 17

Current Value New Value

Profile pftMGCP-1

Call Agent: 127.0.0.1:2727

Call Agent Profile Generic

Disconnect Threshold (0..1,410,065,408): 8

Suspicion Threshold (0..1,410,065,408): 6

Retransmit Delay (100..4000 milliseconds): 300

Max. Retransmit Delay (100..4000 milliseconds): 3000

Local UDP Port (1..65535): 2427

DSCP Setting (0..63): 35

VLAN P-bits (0..7): 4

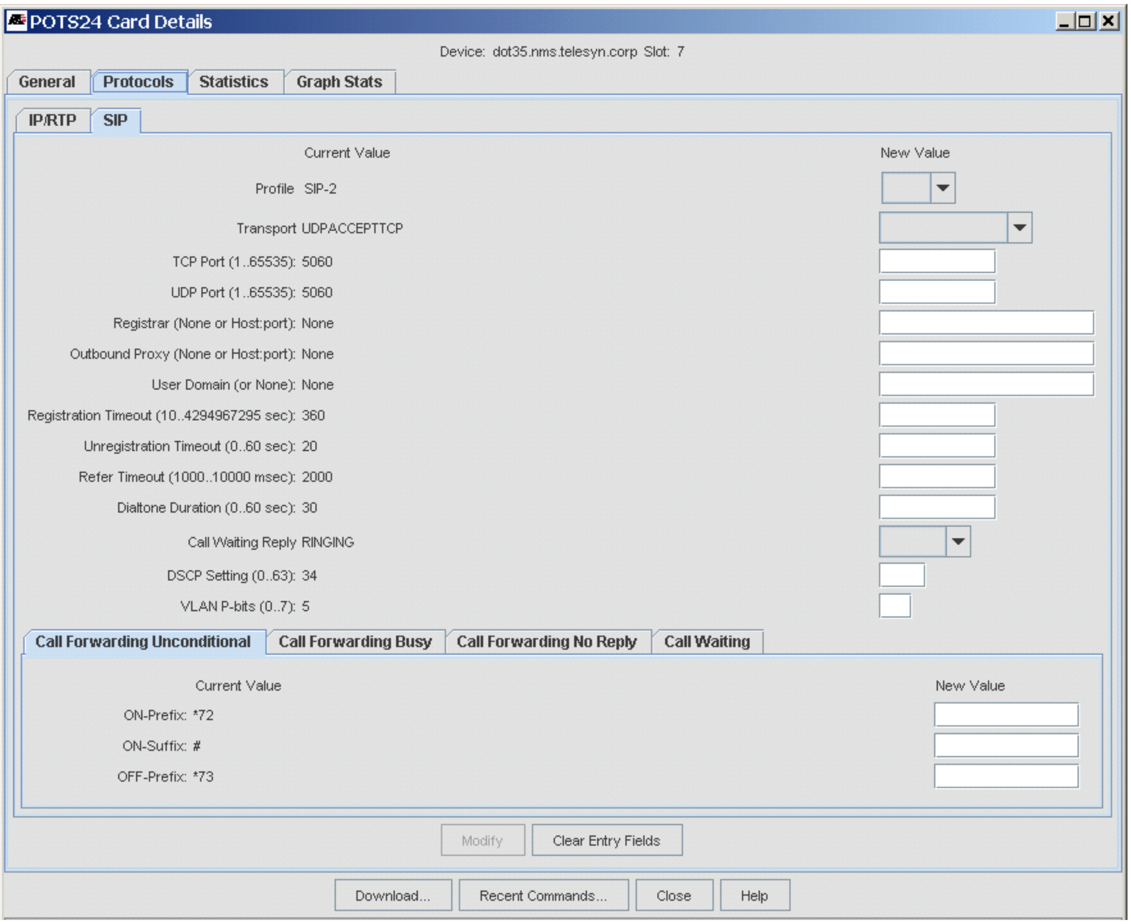
FIGURE 13-11 POTS24 Card - Protocols/MGCP Tab

TABLE 13-7 POTS24 Card Details - Protocols Tab for MGCP

Field/Button	Description
Profile	The profile that has been applied to the card.
Call Agent (or None)	The IP address of the network call agent that the card will communicate with.
Call Agent Profile	Generic or vendor-specific call agent profile.

TABLE 13-7 POTS24 Card Details - Protocols Tab for MGCP (Continued)

Field/Button	Description
Disconnect Threshold	Also known as Max2 in RFC 3435, this is the number of unacknowledged packet retransmissions towards the call agent before beginning a disconnect procedure if there are no other call agent addresses available. Once this threshold is exceeded, the POTS24 card will be in the FAILED state. The default value is **7**.
Suspicion Threshold	Also known as Max1 in RFC 3435, this is the number of unacknowledged packet retransmissions toward the call agent that are allowed before suspecting that the call agent is unreachable, which triggers the MGCP application running in the POTS24 card to use alternate addresses for the agent or initiate a new DNS query to verify the call agent address. The default value is **5**.
Retransmit Delay (100..4000 ms)	The initial delay before any packet retransmission is done towards the call server. The default value is **200 milliseconds**.
Max. Retransmit Delay (100..4000 ms)	Also known as RTO-MAX in RFC 3435, this is the maximum amount of time to wait for an acknowledgement from the call agent before retransmitting a packet. The default value is **4000 milliseconds**.
UDP Port	Specifies the UDP (User Datagram Protocol) port the MGCP application in the POTS24 card will use for receiving packets. The default value is **2427**.
DSCP Settings (0..63)	The DSCP (Differentiated Services Code Point, RFC 2474) value for MGCP packets transmitted from the POTS24 card The default value is **34**.
VLAN P bits (0..7)	The 802.1p priority bit setting for MGCP packets transmitted from the POTS24 card. The default value is **5**.
Modify	Activated when a value has been changed. WHen selected, makes the changes to the card.
Clear Entry Fields	Clears all changed values
Download	Brings up the Download Software window. Refer to Controlling Card Software (Download and Restart).



Device: dot35.nms.telesyn.corp Slot: 7

Current Value New Value

Profile SIP-2

Transport UDPACCEPTTCP

TCP Port (1..65535): 5060

UDP Port (1..65535): 5060

Registrar (None or Host:port): None

Outbound Proxy (None or Host:port): None

User Domain (or None): None

Registration Timeout (10..4294967295 sec): 360

Unregistration Timeout (0..60 sec): 20

Refer Timeout (1000..10000 msec): 2000

Dialtone Duration (0..60 sec): 30

Call Waiting Reply RINGING

DSCP Setting (0..63): 34

VLAN P-bits (0..7): 5

Current Value New Value

ON-Prefix: *72

ON-Suffix: #

OFF-Prefix: *73

FIGURE 13-12 POTS24 Card - Protocols/SIP Tab

TABLE 13-8 POTS24 SIP Attributes - (Defaults are in Bold)

POTS24 Card Attribute	**Description**
Profile	The Profile that has been applied to the card
Transport	The Transport type of the outgoing messages. When set to *UDP Accept TCP*, the IP Phone will accept incoming TCP messages. (**TCP**)
TCP Port	The TCP port on which the Stack listens. (**5060**)
UDP Port	The UDP port on which the Stack listens (**5060**)
Registrar (Host port)	The Registrar IP address or domain name. If this parameter is not set, Registration messages will not be sent. **NULL** (The number of the Port on which the Registrar listens)
Outbound Proxy (Host Port)	The IP address of the outbound Proxy. If this parameter is set, all outgoing messages (including Registration messages) will be sent to this Proxy. The outboundProxyHostName can be used for setting the IP address or the DNS name that the call application can parse **NULL** (The number of the Port on which the outbound Proxy listens)
User Domain	This domain name will be sent in the From header of outgoing Invite messages
Registration Time-out	The time-out (in seconds) for sending Proxy Re-registration requests **3600**

TABLE 13-8 POTS24 SIP Attributes - (Defaults are in Bold) (Continued)

POTS24 Card Attribute	Description
Unregistration Time-out	This parameter is relevant for unregistration requests that are sent as part of the IP Phone Toolkit shutdown process. The time-out (in seconds) indicates the time interval to wait for a reply after sending an unregister request before completing the shutdown process. If the time-out expires before a reply has been received, the shutdown process will be completed. If a reply is received before the time-out expires, the IP Phone Toolkit will respond accordingly and then complete the shutdown process. **20**
Refer Time-out	The time-out (in milliseconds) for waiting for Notify after sending Refer, before disconnecting the call-leg **2000**
Dialtone Duration	Duration of Dial Tone signal (in milliseconds) when going off-hook. When the subscriber goes off-hook and time-out expires, Dial Tone will be stopped and the connection will disconnect. 0 indicates an infinite Dial Tone. **3000**
Call Waiting Reply	When the incoming call is a Call Waiting call, this parameter indicates which SIP message will be sent as a reply to the Invite.
DSCP Settings (0..63)	The DSCP (Differentiated Services Code Point, RFC 2474) value for SIP packets transmitted from the POTS24 card. **34**
VLAN P bits (0..7)	The 802.1p priority bit setting for SIP packets transmitted from the POTS24 card. **5**
Call Forwarding Unconditional Sub-tab ON-Prefix ON-Suffix OFF-Prefix	After CFW Unconditional has been activated, incoming calls are forwarded independently of the status of the endpoint.
Call Forwarding Busy Sub-tab ON-Prefix ON-Suffix OFF-Prefix	After CFW Busy has been activated, incoming calls are forwarded only if the endpoint is busy, i.e., all lines are active.
Call Forwarding Busy Sub-tab ON-Prefix ON-Suffix OFF-Prefix	After CFW No Reply has been activated, incoming calls are forwarded only if the endpoint does not answer before a pre-configured time-out.

13.19.4 POTS 24 Statistics Tab

TABLE 13-9 POTS24 Card Details - Statistics Tab for MGCP

Field/Button	Description
MGCP Statistics	Statistics supported for the MGCP application running on the POTS24 card are defined in the ATN SNMP Enterprise MIB. **SentMessages**: The total number of messages sent. This includes both commands and responses. **RcvdMessages**: The total number of messages received. This includes both commands and responses. **LostMessages**: The number of command messages for which responses were not received. **CmdsRetransmitted**: The number of commands that had to be retransmitted. **RcvdBadVersionMessages**: The number of messages received that were discarded due to the presence of an unsupported MGCP version number in the message. **UnrecognizedMessages**: The number of messages received that were discarded because they were unrecognizable as MGCP messages.
Interface Statistics	These are the statistics from the Interface MIB. Refer to the *Software Reference for iMAP Series Switches*.
RMON Statistics	These are the standard Ethernet-based statistics
Name	Defined in the High Capacity RMON MIB (RFC3273 - etherStatsHighCapacityTable)
High Capacity Counts	Name of high capacity counts, for example 63 Octet packets is the total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
Overflow	The number of times the associated counter has overflowed. In iMAP MAP 4.1 these should always be 0.
Reset MGCP Statistics	Resets the MGCP statistics to 0.
Enable RMON Statistics	Activated when the RMON statistics are disabled.
Disable RMON Statistics	Activated when the RMON statistics are enabled.
Reset RMON Statistics	Resets the RMON statistics to 0.
Download	Brings up the Download Software window. Refer to Controlling Card Software (Download and Restart).

TABLE 13-10 POTS24 Card Details - Statistics Tab for SIP

Field/Button	Description
SIP Statistics	Statistics supported for the SIP application running on the POTS24 card are defined in the ATN SNMP Enterprise MIB. **Invites Received / Retransmitted**: The total number of invite messages received and retransmitted. **Non-Invites Received / Retransmitted**: The total number of non-invite messages sent and retransmitted. **Responses Received / Retransmitted**: The number of responses messages received and retransmitted. **Invites Sent / Invite Retransmits Sent**: The total number of invite messages sent and retransmitted. **Non-Invites Sent / Non-Invite Retransmits Sent**: The total number of non-invite messages sent and retransmitted. **Responses Sent / Responses Retransmit Sent**: The number of responses and retransmitted Responses sent
Interface Statistics	These are the statistics from the Interface MIB. Refer to the *Software Reference for iMAP Series Switches*.
RMON Statistics	These are the standard Ethernet-based statistics
Name	Defined in the High Capacity RMON MIB (RFC3273 - etherStatsHighCapacityTable)
High Capacity Counts	Name of high capacity counts, for example 63 Octet packets is the total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
Overflow	The number of times the associated counter has overflowed. These should be 0.
Reset SIP Statistics	Resets the SIP statistics to 0.
Enable RMON Statistics	Activated when the RMON statistics are disabled.
Disable RMON Statistics	Activated when the RMON statistics are enabled.
Reset RMON Statistics	Resets the RMON statistics to 0.
Download	Brings up the Download Software window. Refer to Controlling Card Software (Download and Restart).

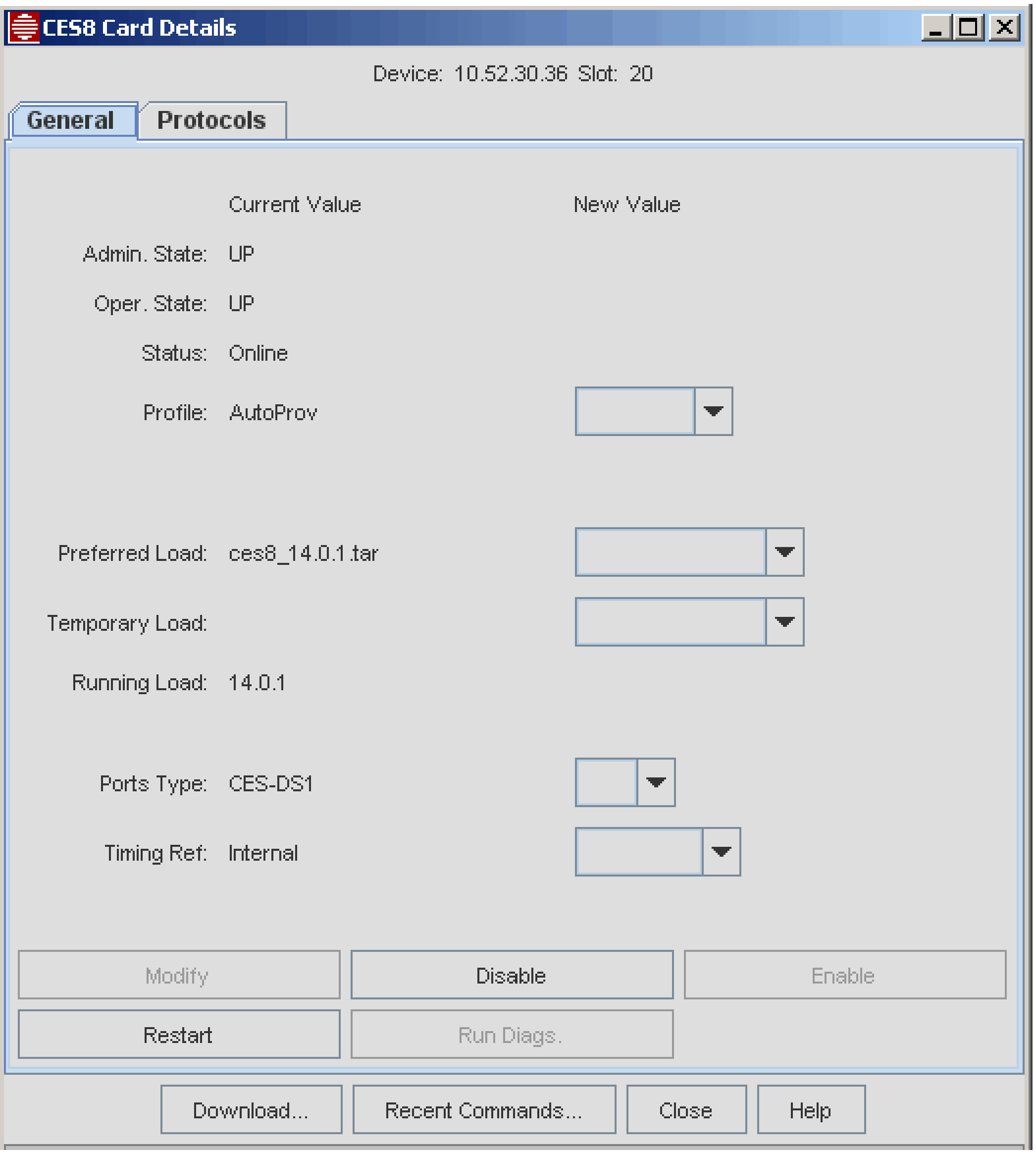
13.19.5 POTS 24 Graph Stats Tab

This is the standard window that allows the user to display the Interface MGCP/SIP, and RMON statistics.

13.20 CES8 Card

The CES8 card provides “Pass-thru” Circuit Emulation Service for both E1 and DS1 circuits.

Note: *The user provisions DS1 or E1 attribute, called the PORTTYPE, at the card level. EI and DS1 ports cannot be provisioned on the same card. Moreover, to modify the PORTTYPE, the user must DISABLE the card. Changing the PORTTYPE effectively destroys the card and creates a new card with the new port types.*



CES8 Card Details

Device: 10.52.30.36 Slot: 20

General | Protocols

	Current Value	New Value
Admin. State:	UP	
Oper. State:	UP	
Status:	Online	
Profile:	AutoProv	
Preferred Load:	ces8_14.0.1.tar	
Temporary Load:		
Running Load:	14.0.1	
Ports Type:	CES-DS1	
Timing Ref:	Internal	

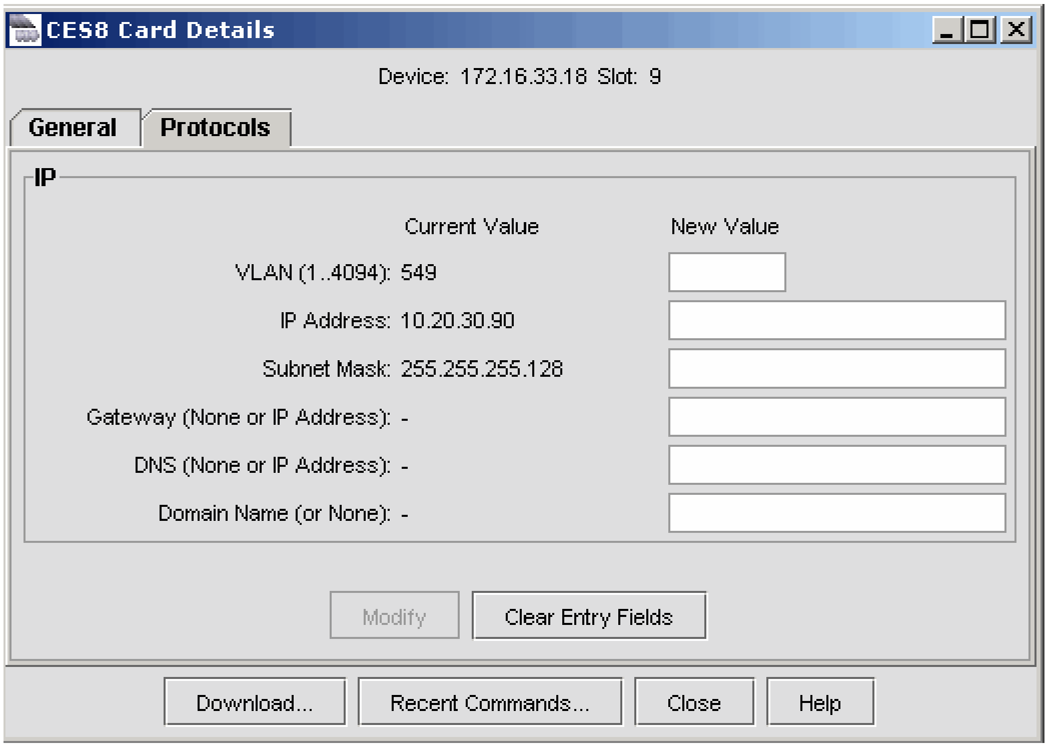
FIGURE 13-13 CES8 Card Details

All the fields for the General tab are the same as for other cards except for the following:

- **Port Type** - This can be DS1 (the default) or E1. Note that the card must be disabled before the Port Type can be changed.
- **Timing Ref.** - The timing reference is where the card will get its clocking reference from. The choices are:
  - INTERNAL - The internal oscillator (locked to a timing signal from the active CFC)
  - A "self-timed" DS1/E1 port physical interface
  - A "self-timed" Pseudo-span (using RTP-based derived, adaptive timing)

The buttons for the CES8 card are similar to other cards, while noting the following:

- **Restart** - Needed when a different load is being used.
- **Run Diags**. - Runs a set of diagnostics. The card must be disabled first. If there are failures, there are messages and logs that can be accessed using the Log Manager.



Device: 172.16.33.18 Slot: 9

IP

	Current Value	New Value
VLAN (1..4094):	549	
IP Address:	10.20.30.90	
Subnet Mask:	255.255.255.128	
Gateway (None or IP Address):	-	
DNS (None or IP Address):	-	
Domain Name (or None):	-	

FIGURE 13-14 CES8 Card Details- Protocols Tab

The Protocols tab is used to fill in the interface attributes of the DS1 card. The only required fields are the VLAN, IP Address, and Subnet mask values, and these must have valid entries or a Set Card Failed window appears.

Note: An IP Interface is required before any DS1/E1 ports can be provisioned for CES.

For details on these fields, refer to the *Software Reference for iMAP Series Switches*. For information on how the CES8 card configuration is datafilled by the NMS, refer to Circuit Emulation Service.

13.21 NTE8 Card

The NTE8 card can be contrasted with the CES8; while the CES8 extends the DS1/E1 network over ethernet facilities, the NTE extends the ethernet network over DS1/E1 facilities.

Note: The user provisions DS1 or E1 attribute, called the PORTTYPE, at the card level. To modify the PORTTYPE, the user must DISABLE the card. Changing the PORTTYPE effectively destroys the card and creates a new card with the new port types.

All the fields for the General tab are the same as for other cards except for the following:

- **Port Type** - This can be DS1 (the default) or E1. Note that the card must be disabled before the Port Type can be changed.
- **Timing Ref.** - The timing reference is where the card will get its clocking reference from. The choices are:
  - INTERNAL - The internal oscillator (locked to a timing signal from the active CFC)
  - A “self-timed” DS1/E1 port physical interface

The buttons for the NTE8 card are similar to other cards, while noting the following:

- **Restart** - Needed when a different load is being used.
- **Run Diags**. - Runs a set of diagnostics. The card must be disabled first. If there are failures, there are messages and logs that can be accessed using the Log Manager.

13.22 ADSL24A, ADSL24B, and ADSL2AE Card

The ADSL24 can be deployed for Annex-A and Annex-B. The ADSL24AE card is also available. Refer to the *Allied Telesis iMAP Component Specification* for details on the card, and the *Software Reference for iMAP Series Switches* for details on provisioning. Otherwise the provisioning GUIs are similar.

13.23 PAC24A, PAC24C Card

The PAC24A and PAC24C cards have the functionality of the ADSL24A card and the POTS24 card onto one card. (For the POTS function, splitters are included.) However, from the provisioning viewpoint, these are still treated as separate cards and so the provisioning GUIs do not change.

Note: The one area where provisioning is combined on the two cards is when the card is provisioned on the Customer Triple Play form; if the user configures the ADSL part, the POTS part is automatically filled in where applicable. Refer to Add New Triple Play Customer - Four Examples.

13.24 EPON2 Card

The NMS can be used to configure the Gigabit Ethernet EPON2 card.

Each EPON2 card has 2 epon interfaces (epon:s.0 and epon:s.1, where s is the card slot number), that can connect with up to 32 ONUs, for a total of 64 ONUs per card. The ONU interfaces are identified as onu:<slot>.<port>.<onuId>, and are thought of as residing on the iMAP, even though they are physically on the ONU device.

Provisioning an EPON2 card is similar to provisioning other cards. Select an iMAP device, and bring up the Card Management window. Select an unprovisioned card slot and click on Create.

13.25 VDSL24 Card

Very high data rate digital subscriber line (VDSL) is a next-generation of high-speed DSL technology that allows faster data rates than the iMAP 9000 ADSL SMs.

The two cards that support VSDL are the VDSL24-A and VDSL24-B, with the following attributes:

- The cards have the **same** software load but support ADSL annex A and annex B by card type.
- Each port can operate in VDSL mode or ADSL annex-A/annex-B mode.

13.26 ADSL48A/B Card

The ADSL is a double-width card and so there are restrictions on where it can be installed (refer to the iMAP Component specification for details). The form for creating the card is standard, and when the card is created the Card Management table shows which two slots the card occupies.

13.27 Viewing Card Details for the iMAP 9100

The card details form is the same as for other iMAP devices with the following exceptions:

The CFC12 card is always in simplex mode and therefore cannot be enabled, disabled, or destroyed, unless the user wishes to drop service, usually during an upgrade.

13.28 GE24POE

The GE24POE card is unique to the SBx3100, and can be loaded in any slot in the SBx3100 chassis except for the CFC slots. Refer to Power Over Ethernet (POE) Management on SBx3100.

13.29 XE Cards (XE1, XE1S, XE4, XE6SFP, and XE6)

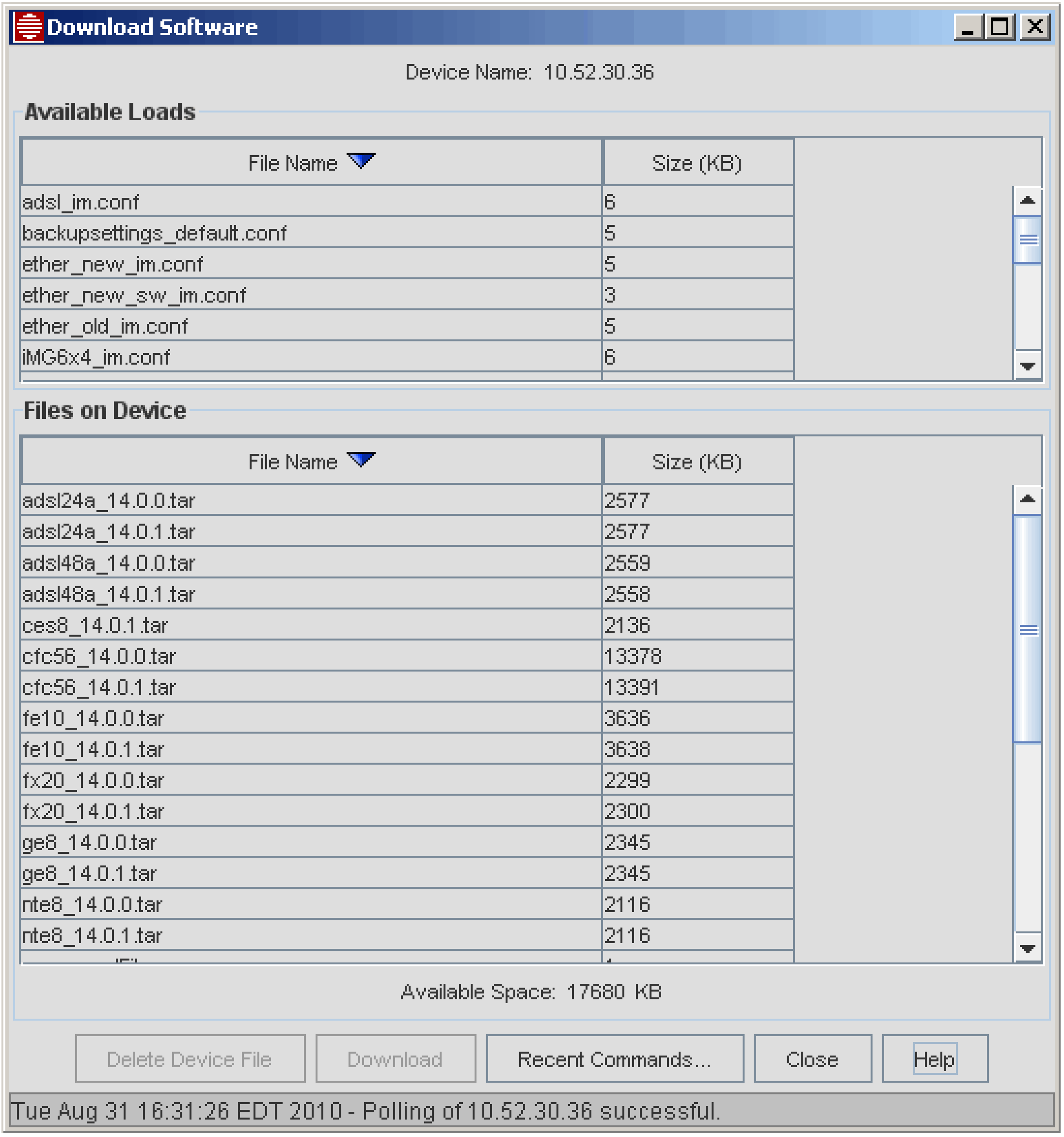
The XE1 card on the iMAP provides a 10GE link between 10G products. The XE4 and XE6SFP cards, unique to the SBx3100, provides four and six of these ports. The XE6 card, used in the iMAP 9700 and 9810 products, provides six of these ports. All have a general tab and allow for Enable, Disable, Restart, and Run Diags. Note that since these cards provide a high-bandwidth interface usually involving connections to upstream devices, care should be taken before disabling this cardtype.

13.30 GE24 Cards (GE24SFP, GE24POE, GE24RJ, GE24BX)

At the card level, all of the Card Details forms have similar functions, with the GE24SFP, GE24POE, and GE24RJ for the SBx3100 and the GE24BX for the iMAP. The GE24POE provides the Power over Ethernet service and is described in Power Over Ethernet (POE) Management on SBx3100. The GE24RJ is the same as the GE24POE but does not provide POE service.

13.31 Controlling Card Software (Download and Restart)

The **Card Details** window includes a Download button that brings up the Download software window. This window displays the current files (and their size) on the FLASH of the card, the available space, and the available loads. Figure 13-15 shows this window and Table 13-11 shows the fields/options available.



Device Name: 10.52.30.36

Available Loads

File Name	Size (KB)
adsl_im.conf	6
backupsettings_default.conf	5
ether_new_im.conf	5
ether_new_sw_im.conf	3
ether_old_im.conf	5
iMG6x4_im.conf	6

Files on Device

File Name	Size (KB)
adsl24a_14.0.0.tar	2577
adsl24a_14.0.1.tar	2577
adsl48a_14.0.0.tar	2559
adsl48a_14.0.1.tar	2558
ces8_14.0.1.tar	2136
cfc56_14.0.0.tar	13378
cfc56_14.0.1.tar	13391
fe10_14.0.0.tar	3636
fe10_14.0.1.tar	3638
fx20_14.0.0.tar	2299
fx20_14.0.1.tar	2300
ge8_14.0.0.tar	2345
ge8_14.0.1.tar	2345
nte8_14.0.0.tar	2116
nte8_14.0.1.tar	2116

Available Space: 17680 KB

Tue Aug 31 16:31:26 EDT 2010 - Polling of 10.52.30.36 successful.

FIGURE 13-15 Download Software Window

Caution: For the devices that will receive downloads, do not set their telnet idle session time-out to any value less than 6 minutes. This minimum is needed to ensure the NMS is aware the download is complete and can proceed with any further steps.

TABLE 13-11 Download Software Window Fields/Buttons

Field/Button	Description
Available Loads	This panel lists the loads available and their size. Selecting a load activates the Download button to allow a file to be downloaded. Once a file is downloaded, the user returns to the Card Details window and presses the Restart button to reboot the card and make the downloaded file the current load. *Note: Before downloading a file, ensure there is enough space on the card to accept the new load. Otherwise an error message will appear. Also, the user must have the Preferred Load or (usually for upgrade) Temporary load set on the card to make the card load with the desired load file.* Controlling files requires a knowledge of how software loads are controlled on the CFC and Service Module (SM) cards. In most cases the SM loads are on the CFC cards, and when the CFC restarts the SM loads are downloaded to the SM cards. Refer to the *Software Reference for iMAP Series Switches* for more details. *Note: The NMS cannot distinguish annex A from annex B for ADSL24 cards (It can distinguish between them for ADSL16 however and it doesn't need to for other card types). Users need to know which annex their cards are. (Files have to be downloaded before they will appear in the preferred load and temporary load picklists.) The annex a file is adsl24_*.tar and the annex b file is adsl24xb_*.tar.*
Files on Device	This panel lists the files currently on the device and their size. Below this list is the space still available in FLASH memory. Clicking on a file activates the **Delete** Device File button and, after a confirmation, deletes the file from the FLASH memory.
Delete Device File	This deletes a file that has been highlighted in the **Files on Device** panel. Deleting a file from FLASH requires knowledge of the status of files (Preferred, Temporary), and must be coordinated with the Details window to ensure the correct load is used when the card restarts.
Download	This downloads a file that has been highlighted in the **Available Loads** panel.

13.32 Overview of Provisioning Data, Profiles, and Card States

Provisioning of cards/ports means to add, modify or delete the card and port information stored on the iMAP devices and to add or remove the physical cards. Provisioning these cards involves the following:

- **Provisioning Data** - The provisioning data itself consists of:
  - States - These determine whether the card or port can be placed in service and if so whether it can process data.
  - Attributes - These are the characteristics of the card or port, usually to optimize the processing of data.
- **Persistence** - This is the ability of the provisioning data to survive changes such as a reboot of the shelf or the removal of a card.
- **Pre-provisioning** - The user has the option of creating a card and having it in the database prior to inserting the card.

Controlling these is done through the use of profiles, operational states, and provisioning modes.

In **Manual Provisioning Mode**, provisioning data must be explicitly created and modified. The data is persistent over reboots and restarts of the device and the removal of the card.

It is important to note that insertion of a card when in the **Manual Provisioning Mode** does **not** create/provision the card in the database; this must be done using the **Create Card** button.

In **Automatic Provisioning Mode**, when hardware is discovered in a slot where there is no prior provisioning, the cards and ports are automatically provisioned. This discovery occurs when:

- The card is inserted into a slot
- The card is already inserted and the device reboots
- The system mode is changed from manual to automatic

Note: *The default mode for the iMAP devices is Automatic Provisioning Mode, and the mode can be changed through the Card Details screen.*

A **profile** is a template that contains the provisioning data. There is one only one profile, called AUTOPROV (for Auto-provisioning), which contains at first the factory defaults, but any or all attributes can be changed. This is the profile used for the Auto Provisioning Mode.

When the system is first initialized, the system's PROVMODE is set to AUTO. Profiles can then be created, viewed, and set.

Note: *Modification of a profile does not change the attributes of a card/port that has already been provisioned.*

Administrative and Operational States determine whether the card or port is available for service and if so whether service is being provided;

- The **Administrative State** is controlled by the user and can be set to either UP (available for service) or DOWN (Not available for service). Control of this state is through the **Create Card** window.
- The **Operational State** is either UP (providing service) or DOWN (not providing service). This state is not user controllable but does depend on the Administrative State:
  - If the Administrative State of a card is UP, the Operational State will be UP if the card/port can provide service.
  - If the Administrative State is DOWN, the Operational State will always be DOWN.

Note: *The one exception to these rules is the FC7 and FM7, which are always in an operational state of UP.*

13.33 Power Over Ethernet (POE) Management on SBx3100

To monitor the actual power usage of the POE cards on the SBx3100, there is a menu item in the physical device pull-down, as shown in the following figure.

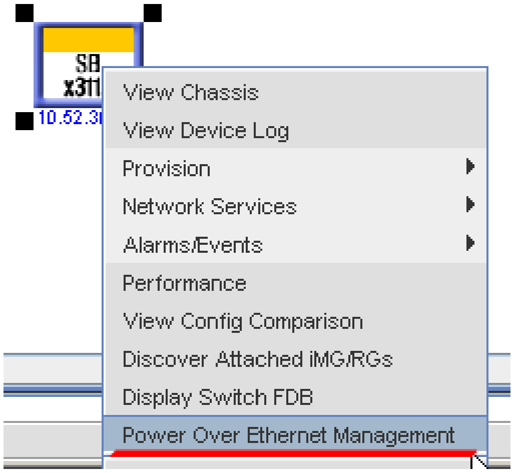
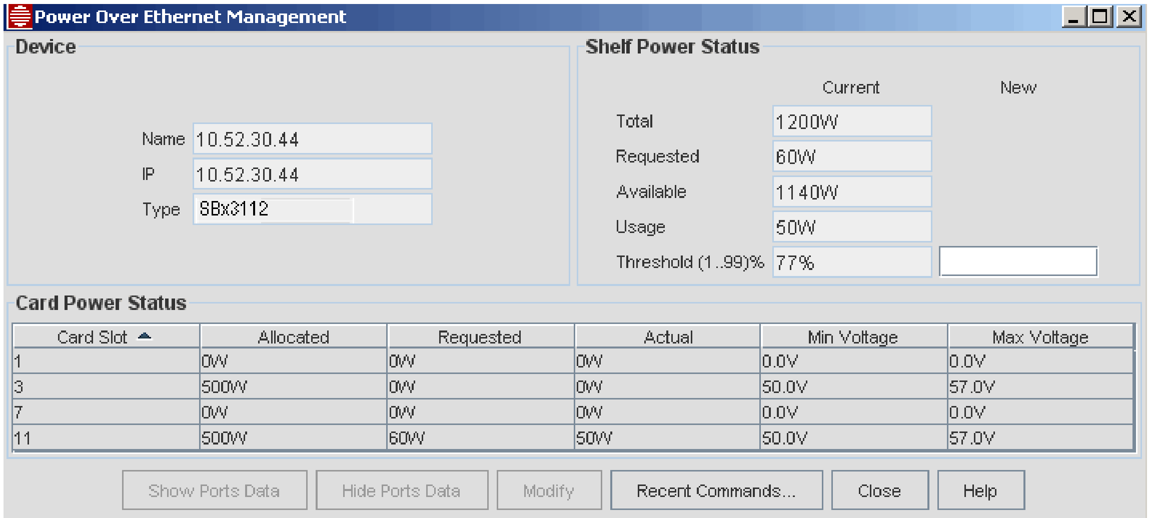


FIGURE 13-16 SBx3100 Pull-down for POE Management

This will launch a separate NMS window that will show the overall power settings for the shelf. This window will show each POE card and how much power is allocated to it, requested by it, and the actual usage. In this way the customer can manage the power distribution across the cards. Refer to the following figure.



Name	10.52.30.44
IP	10.52.30.44
Type	SBx3112

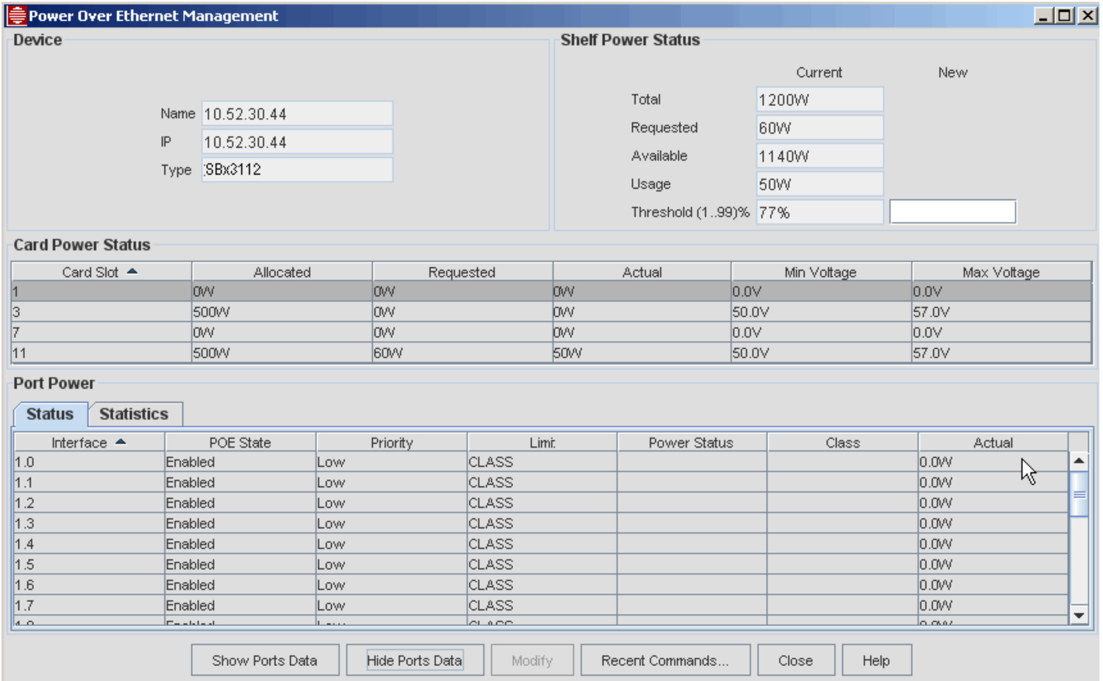
	Current	New
Total	1200W	
Requested	60W	
Available	1140W	
Usage	50W	
Threshold (1..99)%	77%	

Card Slot	Allocated	Requested	Actual	Min Voltage	Max Voltage
1	0W	0W	0W	0.0V	0.0V
3	500W	0W	0W	50.0V	57.0V
7	0W	0W	0W	0.0V	0.0V
11	500W	60W	50W	50.0V	57.0V

FIGURE 13-17 Power Over Ethernet Management Form - Cards

Note: The Shelf Threshold for the shelf can only be set from Power Over Ethernet Management Form.

By selecting one/multiple cards and selecting **Show Ports Data**, the user can display all of the port -specific information for the card(s) that are selected. This will show the customer the way in which power is distributed among the ports. Refer to the following figure.



Name	10.52.30.44
IP	10.52.30.44
Type	SBx3112

	Current	New
Total	1200W	
Requested	60W	
Available	1140W	
Usage	50W	
Threshold (1..99)%	77%	

Card Slot	Allocated	Requested	Actual	Min Voltage	Max Voltage
1	0W	0W	0W	0.0V	0.0V
3	500W	0W	0W	50.0V	57.0V
7	0W	0W	0W	0.0V	0.0V
11	500W	60W	50W	50.0V	57.0V

Interface	POE State	Priority	Limit	Power Status	Class	Actual
1.0	Enabled	Low	CLASS			0.0W
1.1	Enabled	Low	CLASS			0.0W
1.2	Enabled	Low	CLASS			0.0W
1.3	Enabled	Low	CLASS			0.0W
1.4	Enabled	Low	CLASS			0.0W
1.5	Enabled	Low	CLASS			0.0W
1.6	Enabled	Low	CLASS			0.0W
1.7	Enabled	Low	CLASS			0.0W

FIGURE 13-18 Power Over Ethernet Management Form - Ports

14. Port Management - iMAP Devices

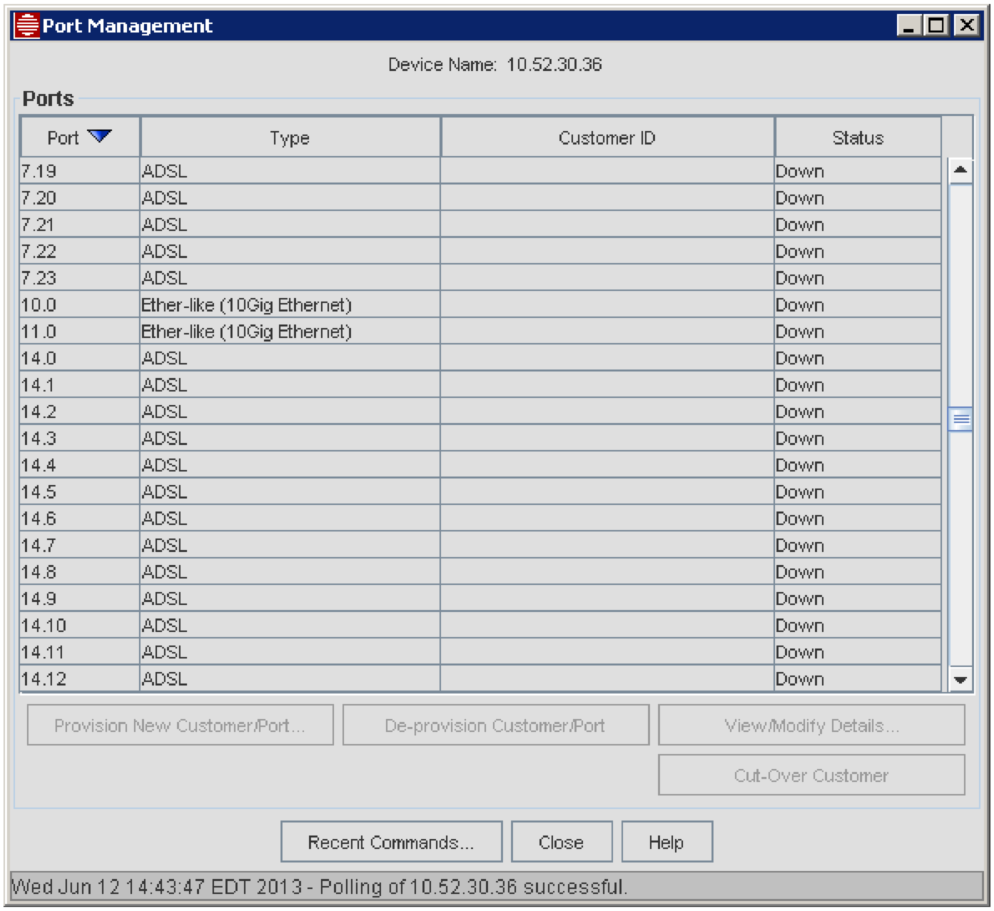
Port Management for iMAP devices provides a of a device’s configuration in table format. The table is updated in real-time as you make changes to the device’s ports. You can provision a device’s ports directly from the **Port Management** window.

The following buttons always appear on the **Port Management** window:

- **Recent Commands** - Opens the Recent Commands window, a listing of the CLI commands and responses for the previous operation in the Port Management application. The user has the option to copy this to a Clipboard and then paste it into another file for record keeping.
- **Close** - Closes the window.
- **Help** - Opens the context-sensitive help file.

To access Port Management:

1. Do one of the following in the **Network Objects** panel:
   - Go to **Network Maps** > **Physical Network**. In the **Physical Network** screen, select the device.
   - Go to **Network Inventory** > **Nodes**. In the **Nodes** screen, select the device.
2. Go to **Operations** > **Provision** > **Port Management**. The **Port Management** window appears.



Device Name: 10.52.30.36

Port	Type	Customer ID	Status
7.19	ADSL		Down
7.20	ADSL		Down
7.21	ADSL		Down
7.22	ADSL		Down
7.23	ADSL		Down
10.0	Ether-like (10Gig Ethernet)		Down
11.0	Ether-like (10Gig Ethernet)		Down
14.0	ADSL		Down
14.1	ADSL		Down
14.2	ADSL		Down
14.3	ADSL		Down
14.4	ADSL		Down
14.5	ADSL		Down
14.6	ADSL		Down
14.7	ADSL		Down
14.8	ADSL		Down
14.9	ADSL		Down
14.10	ADSL		Down
14.11	ADSL		Down
14.12	ADSL		Down

Wed Jun 12 14:43:47 EDT 2013 - Polling of 10.52.30.36 successful.

FIGURE 14-1 Port Management

TABLE 14-1 Port Management

Field/Button	Description
Device Name	The name given to the device in the Managed Objects property table.
Port	The slot.port in the iMAP device.
Type	Allowed port types are ADSL, SHDSL, Ether-like, POTS, DS1, E1, VDSL, and ATMBOND.
Customer ID	A unique ID to identify the port. For example, the subscriber's telephone number. For rules on DS1/E1 customer IDs, refer to "Circuit Emulation Service" on page 623. Note: Do not use the asterisk (*) character in customer IDs. Customer IDs with * in the string will not appear properly in searches.
Status	The status of the port that follows from the boolean AND of the Administrative State and Operational State (only if both are UP is the Status UP).
Provision New Customer/Port	Enabled when you select a port that does not have a Customer ID. Opens the Provision New Triple Play Customer form.
De-Provision Customer/Port	Deletes the Customer ID and sets the Administrative State to DOWN. The status becomes OFFLINE. This operation also sets the port back to the AutoProv settings, removes any classifiers on the port, removes VCs 1-3 from the port, and sets the VLAN back to Untagged:1 Tagged None.
View/Modify Details	Enabled when a port is selected. Opens the Port Management details form.

There are three versions of the Port Management window and Port Management details form:

1. View Only
   - The Port Management screen excludes the Provision and De-Provision buttons.
   - The Port Management details form excludes the fields/buttons that allow values or states to be changed.
2. Provision - The same as View Only, but includes the Provision and De-Provision buttons.
3. Setting - The same as Provision, but includes the fields/buttons that allow values or states to be changed.

Control of these versions is though the NMS Security Manager settings.

Note: Provisioning ports can involve defining the attributes of a single port or more than one port. With the CES8 and NTE8 card, two ports are provisioned on the same form when configuring the two endpoints of a DS1/E1 connection. Provisioning dual DS1/E1 ports is explained in more detail in "Circuit Emulation Service" on page 623 and "NTE8 Dual Circuit Provisioning" on page 653.

Note: Although many types of ports can be provisioned, they are all done through the two forms that define the services for a port, the Provision New Triple Play Customer Form, and the Provision New DS1/E1 Port Form, which can apply to the CES8 or the NTE8. This section explains these form and their fields; for an overview of the panels and fields that are used for various services, refer to "Customer Management" on page 615.

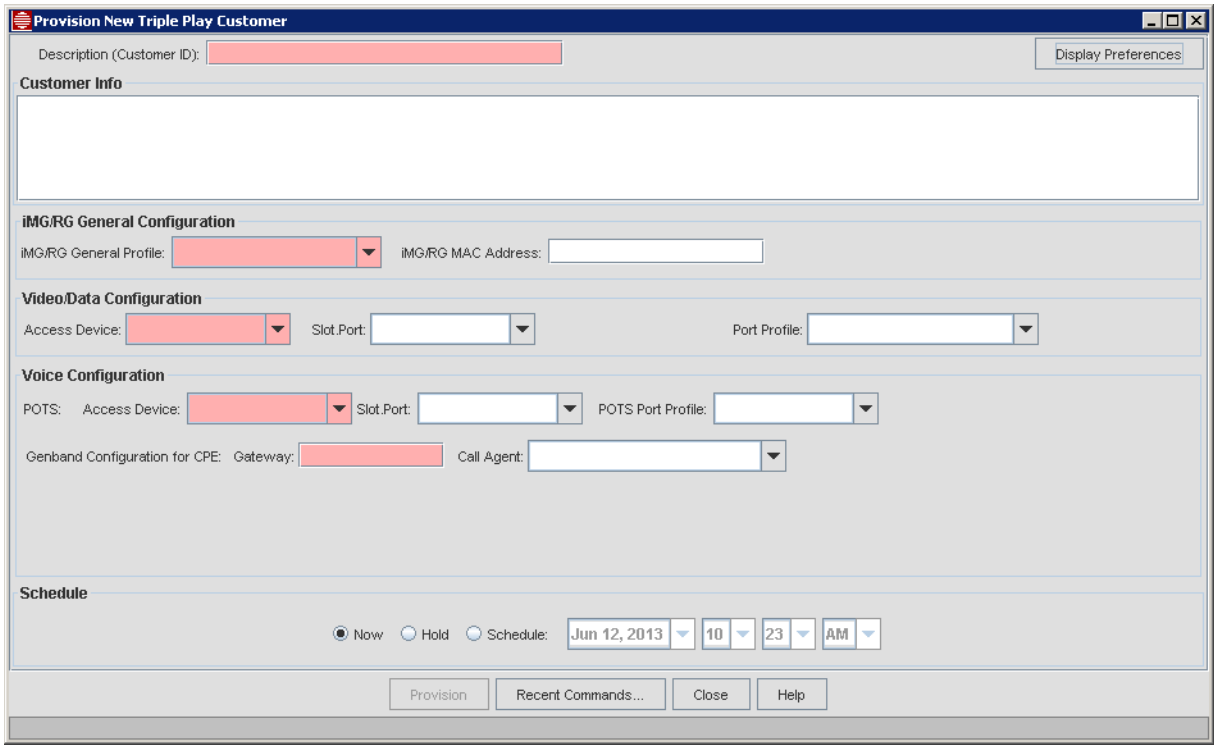
Note: For the ADSL48A card, the port numbers go from 0 to 47, and the card number remains at the lower slot number for ports 24 to 47.

Note: In the Port Management window, an AtmBond shows up as type "ATMBOND". The bonded port does not appear in this window.

14.1 Provision a New Triple Play Customer

To provision a new Triple Play customer from Port Management:

1. Do one of the following in the **Network Objects** panel:
   - Go to **Network Maps** > **Physical Network**. In the **Physical Network** screen, select the device.
   - Go to **Network Inventory** > **Nodes**. In the **Nodes** screen, select the device.
2. Go to **Operations** > **Provision** > **Port Management**. The **Port Management** window appears.
3. Select a port that is not provisioned yet. The port can be any type other than xDSL, CES8, NTE8 or EPON.
4. Click **Provision New Customer/Port**. The **Provision New Triple Play Customer** form appears with required fields highlighted.



● Now ○ Hold ○ Schedule: Jun 12, 2013 10 23 AM

FIGURE 14-2 Provision New Triple Play Customer

TABLE 14-2 Provision New Triple Play Customer

Panel	Field/Button	Description
Top of Form	Display Preferences	Allows you to choose which panels and fields display on the **Provision Port for Triple Play Customer** form. The most common fields appear by default.
	Description (Customer ID)	A way to identify the customer. The name should be descriptive so it can be easily recognized, especially on the Ports table in Network Inventory. The name should be unique to differentiate it from other customers, but in some configurations the name can apply to more than one port, such as DS1/E1 ports for CES. Refer to "Circuit Emulation Service" on page 623 and "Naming Convention for Customer IDs (Triple Play Form)" on page 780.
	Customer Info.	Text field to include more details about the customer.
iMG/RG General Configuration	iMG/RG General Profile	A pull-down with the pre-defined general profiles for the RG. When provisioning the RG the user should have already defined all the RG profile types. Refer to "iMG General Profile" on page 702.
	iMG/RG MAC Address	The MAC address that uniquely identifies the RG device.

TABLE 14-2 Provision New Triple Play Customer

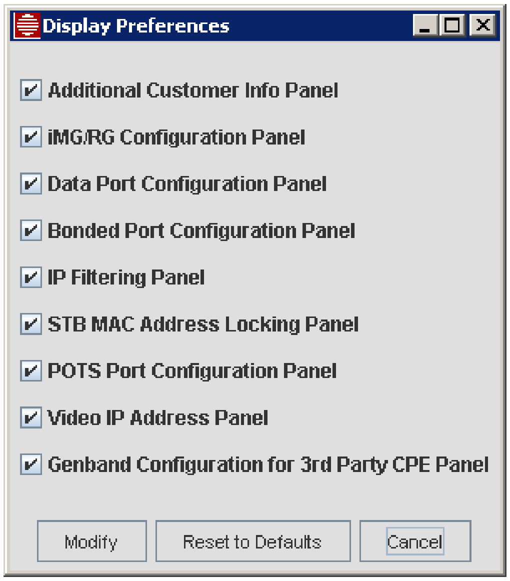
Panel	Field/Button	Description
Video/Data Configuration	Access Device	A drop-down list of all the iMAP Devices that have ports that can support some (or all) aspects of triple play
	Slot Port	Once the Access Device is chosen, the available ports are on that device are listed in the drop-down list. When a port is chosen the port type appears next to the port in parentheses. The default state of ports on AlliedWare Plus devices has a customer name of 'portx.x.x' for all ports. You must deprovision the port to remove this customer name, then reprovision using the triple-play form to provision a relevant customer name.
	Port Profile	Once the port (and therefore port type) is chosen, the available profiles for that port type appear in the drop-down list. When the port is provisioned, it inherits the attributes of that profile. - If the profile includes a VLAN, the VLAN fields are greyed out. - If IGMP snooping is set to OFF in the profile, MAC lookup cannot be done, so the STB fields are grayed out. - For iMAP and SBx3100 devices, IGMP Snooping is applied to the port. For devices running iMAP software up through release 16.x.x, IGMP Snooping must be enabled system-wide. For devices running software release 17.x.x and higher, IGMP Snooping must be enabled on individual VLANs.
	VLAN Settings	The VLANs to be associated with the port. The Untagged VLAN is the default VLAN (packets with no VLAN tag are given this number VLAN). The port may contain more than one untagged VLAN, with each VLAN number separated by a comma.
	IP Filtering (Allowed Ranges)	Incoming data to the ports (the ingress ports) can be filtered by IP address or a range of IP addresses.
	Allowed STB MAC Addrs	These fields are visible when **STB MAC Address Locking Panel** is checked in Display Preferences. For additional security, optionally enter MAC addresses of the STBs to configure IGMP snooping security on the iMG. Note: These fields only pertain to iMGs running software release 2 or release 3. iMGs running software release 4 or higher will ignore them.
Voice Configuration	POTS	The attributes that support iMAP Devices that have ports that can support the POTS aspect of triple play. Specific attributes are controlled by the POTS Port Profile selected.
	Derived Voice	The attributes for Voice over IP provided by iMG/RGs. Specific attributes are controlled by the Derived Voice Service Profile (RG Voice profile) selected. If the profile specifies GenBand MGCP, then attributes are provided to directly configure the GenBand voice gateway. For GenBand, the NMS does not support TR-008.

TABLE 14-2 Provision New Triple Play Customer

Panel	Field/Button	Description
Bottom of Form	Provision	The ability of the port to provide service. The Administrative State must be up and then the system determines if the port can provide service.
	Close	Cancels the provisioning of the port.

14.1.1 Display Preferences

The **Display Preferences** box allows you to control which panels and fields appear in the **Provision New Triple Play Customer** form. To open the **Display Preferences** box, click **Display Preferences** in the upper right corner of the **Provision New Triple Play Customer** form.



Display Preferences

☑ Additional Customer Info Panel

☑ iMG/RG Configuration Panel

☑ Data Port Configuration Panel

☑ Bonded Port Configuration Panel

☑ IP Filtering Panel

☑ STB MAC Address Locking Panel

☑ POTS Port Configuration Panel

☑ Video IP Address Panel

☑ Genband Configuration for 3rd Party CPE Panel

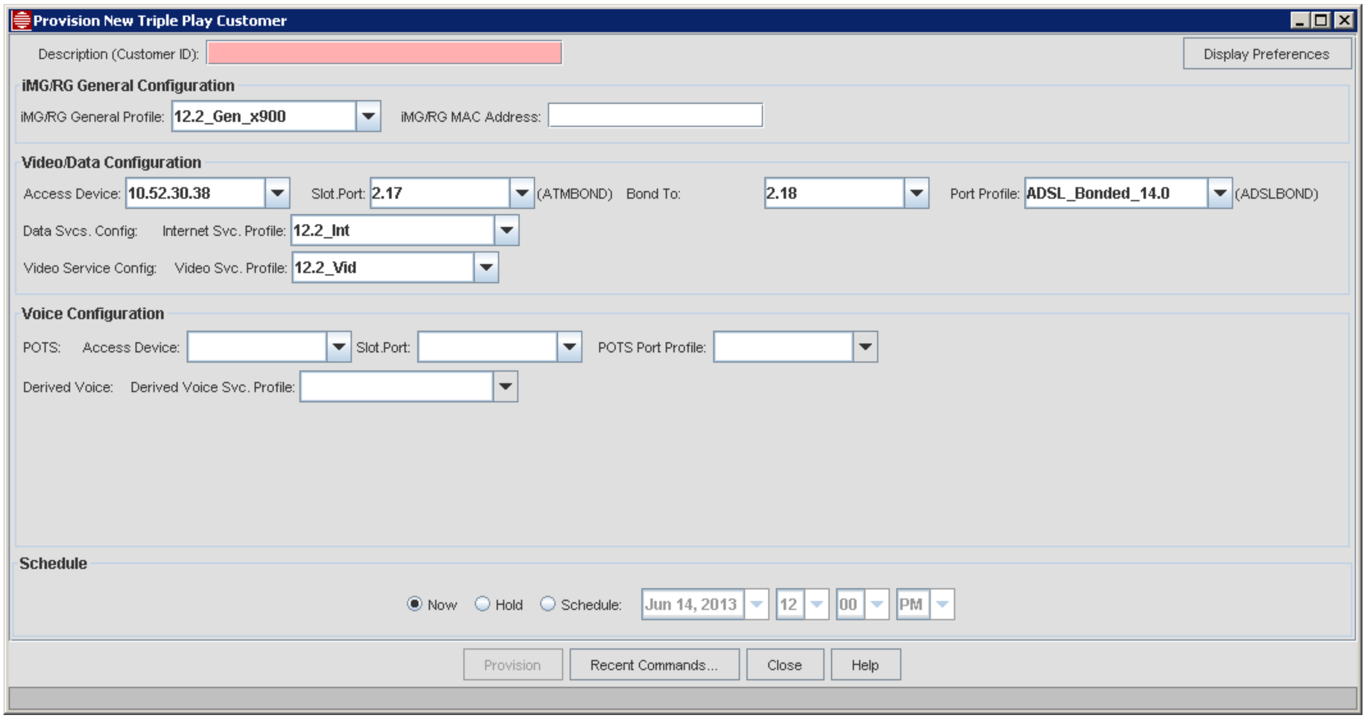
FIGURE 14-3 Display Preferences for the Provision New Triple Play Customer Form

Preferences are on a per-client basis and are automatically saved. Unless you want to change which panels display in the **Provision New Triple Play Customer** form, you do not need to reset them with each new session of the NMS.

14.1.2 Provisioning for ADSL G.Bond

Use the **Provision New Triple Play Customer** form to provision ADSL bonding. In the Display Preferences box, check the box **Bonded Port Configuration Panel** to affect the GUI as follows:

- ADSL-BOND type profiles are included in the port profile selector in addition to the regular ADSL profiles.
- Following the **Slot.Port** field is a new selector field, **Bond To**. It is populated with the other unassigned ports on the same card as the primary port.
- Selecting an ADSL-BOND profile makes the **Bond To** field a required entry.



Provision New Triple Play Customer

Description (Customer ID):

iMG/RG General Configuration

iMG/RG General Profile: 12.2_Gen_x900 iMG/RG MAC Address:

Video/Data Configuration

Access Device: 10.52.30.38 Slot.Port: 2.17 (ATMBOND) Bond To: 2.18 Port Profile: ADSL_Bonded_14.0 (ADSLBOND)

Data Svcs. Config: Internet Svc. Profile: 12.2_Int

Video Service Config: Video Svc. Profile: 12.2_Vid

Voice Configuration

POTS: Access Device: Slot.Port: POTS Port Profile:

Derived Voice: Derived Voice Svc. Profile:

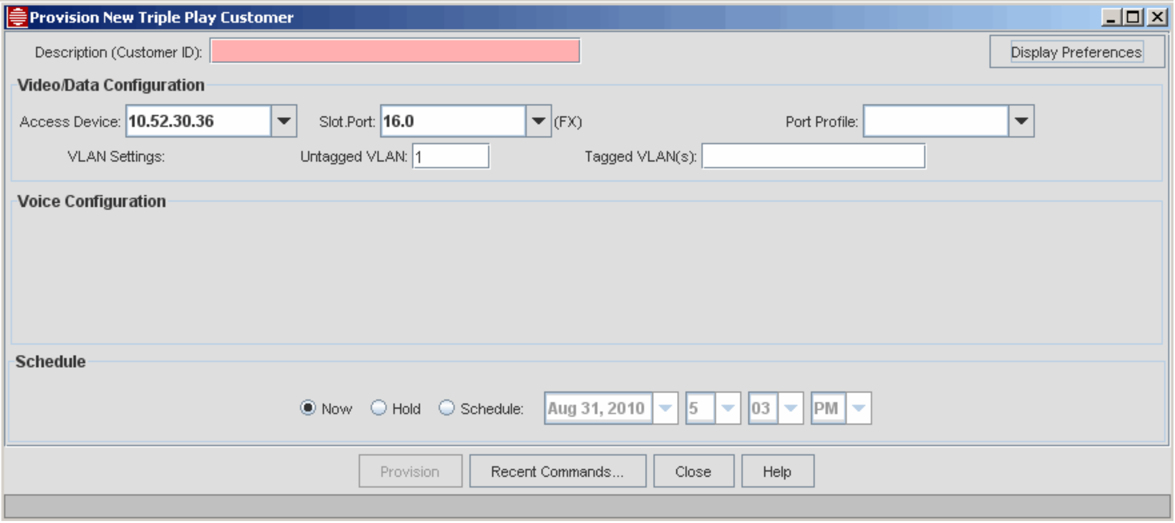
Schedule

● Now ○ Hold ○ Schedule: Jun 14, 2013 12 00 PM

FIGURE 14-4 Triple Play for ADSL Bonded Ports

14.2 Provision New Customer Port for Ethernet

For an ethernet port, a form allows the user to provision a Customer ID and apply a profile so that the port can be placed in service. Refer to the following figure.



Provision New Triple Play Customer

Description (Customer ID):

Video/Data Configuration

Access Device: 10.52.30.36 Slot.Port: 16.0 (FX) Port Profile:

VLAN Settings: Untagged VLAN: 1 Tagged VLAN(s):

Voice Configuration

Schedule

● Now ○ Hold ○ Schedule: Aug 31, 2010 5 03 PM

FIGURE 14-5 Provision New Ether-Like Port

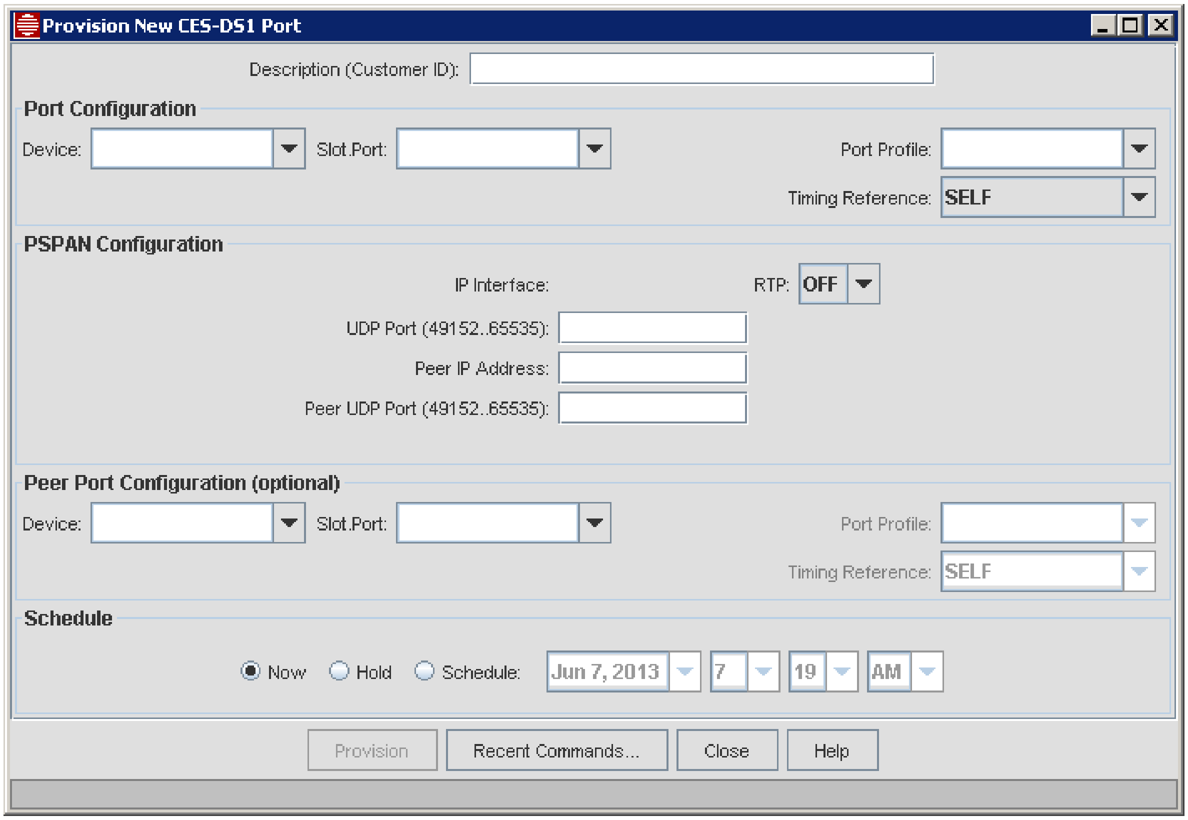
14.3 Provision New Customer/Port for ADSL

Selecting a non-provisioned ADSL port brings up the Triple Play Form that already includes the Access Device and selected port. The form is filled out for services as described in "Provision a New Triple Play Customer" on page 398.

14.4 Provision New CES8-DS1 Port Form

Selecting a non-provisioned port that is a DS1/E1 port and then clicking **Provision New Customer/Port** invokes the **Provision New DS1/E1 Customer** form, as shown in Figure 14-6. This form includes the most important attributes for the port to ensure quality subscriber service. Table 14-3 lists these attributes.

Note: *To provision CES efficiently, use this Provisioning Dialog; this will prevent errors that can occur when changing certain attributes on the DS1 Port Management form.*



Timing Reference: SELF

RTP: OFF

Timing Reference: SELF

● Now ○ Hold ○ Schedule: Jun 7, 2013 7 19 AM

FIGURE 14-6 Provision New DS1 Port Form

TABLE 14-3 **Provision Port for DS1/E1Form**

Panel	Field/Button	Description
Top of Form	Description (Customer ID)	A way to identify the customer. The name should be descriptive so it can be easily recognized, especially on the Ports table in Network Inventory. The name should be unique to differentiate it from other customers, but in some configurations the name can apply to more than one port, such as DS1/E1 ports for CES. Refer to "Circuit Emulation Service" on page 623.

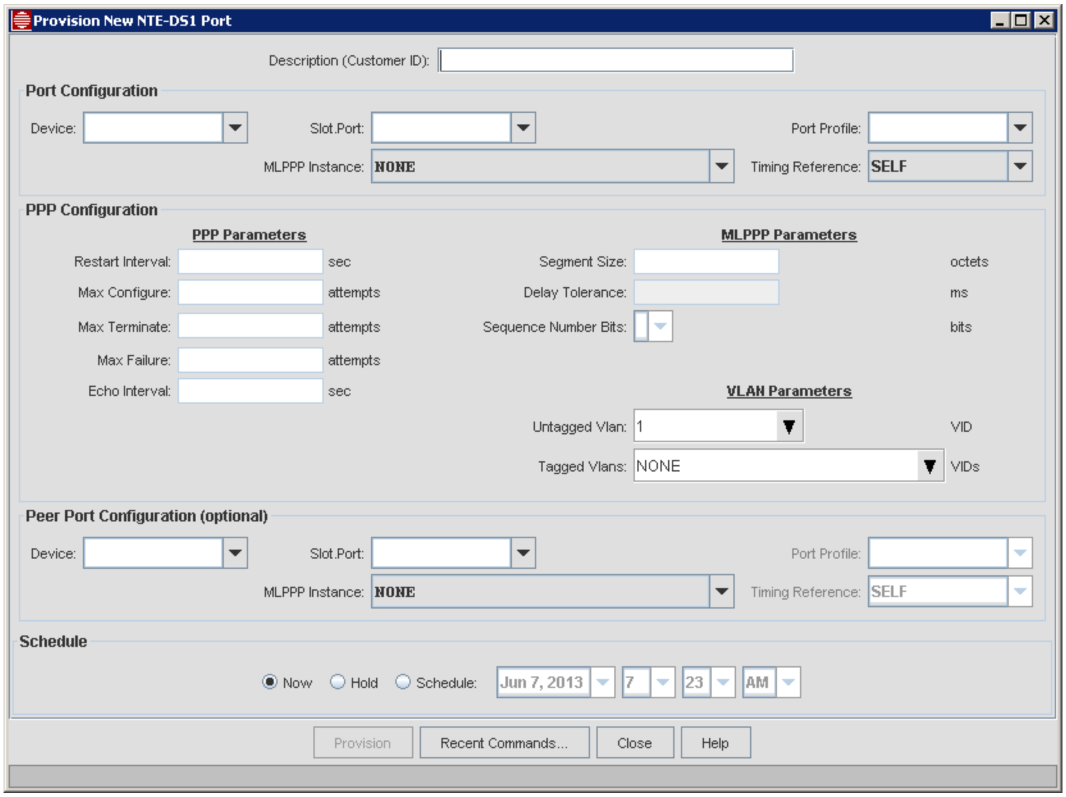
TABLE 14-3 Provision Port for DS1/E1Form

Panel	Field/Button	Description
Port Configuration	Device	A drop-down of all the devices that have CES8 cards configured as DS1 ports (or, if the port is an E1, all the devices that have CES8 cards configured as E1 ports).
	Ports	A drop-down of the ports (card.slot) in the selected device that are DS1 or E1, depending on the port type being configured.
	Port Profile	The available profiles for the port type (DS1 or E1) appear in the drop-down list. When the port is provisioned, it will inherit the attributes of that profile.
	Timing Reference	Where the port will get its clocking reference from. The choices are: - SELF - Itself - CONNECTION -The interface to which it is connected. Note that when this is chosen, the PSPAN automatically has its RTP set to ON, since a PSPAN must be using RTP protocol to be used as a timing reference. - CARD - The "card-level" timing reference.
PSPAN Configuration	IP Interface	The IP interface that has been configured on the card.
	RTP:	Whether RTP timing will be On or OFF. Refer tot he Timing Reference field above.
	UDP port	The UDP port of the near end interface, the local receive ID. Must be unique within an IP address on a card.
	Peer IP Address	The peer IP address of the IP interface the PSPAN is built on. *Note: If the Peer Port is configured, this field is greyed out.*
	Peer UDP Port	Must match the peer's UDPPORT attribute *Note: If the Peer Port is configured, this value is automatically given to the peer port.*
Peer Port Configuration (optional)	Device	The device that contains the peer DS1/E1 port.
	Port	A drop-down of the ports (card.slot) in the selected device that are DS1 or E1, depending on the port type being configured *Note: A peer port can be on a different device or the same device as the port, but cannot be on the same card.*
	Port Profile	The available profiles for the port type (DS1 or E1) appear in the drop-down list. When the port is provisioned, it will inherit the attributes of that profile.
	Timing Reference	Where the port will get its clocking reference from. The choices are the same as for the port.
Bottom of Form	Provision	Enabled only after the minimum number of correct fields have been data filled, and these fields have been data filled with valid values.

14.5 Provision New NTE-DS1 Port Form

Selecting a non-provisioned port that is a DS1/E1 port and then clicking **Provision New Customer/Port** invokes the **Provision New NTE-DS1 Port** form, as shown in Figure 14-6. This form includes the most important attributes for the port to ensure quality subscriber service. Table 14-4 lists these attributes.

Note: To provision the NTE8 efficiently, use this Provisioning Dialog; this will prevent errors that can occur when changing certain attributes on the DS1 Port Management form.



Description (Customer ID):

Port Configuration: Device: | Slot.Port: | Port Profile: | MLPPP Instance: NONE | Timing Reference: SELF

PPP Parameters: Restart Interval: | Max Configure: | Max Terminate: | Max Failure: | Echo Interval:

MLPPP Parameters: Segment Size: | Delay Tolerance: | Sequence Number Bits:

VLAN Parameters: Untagged Vlan: 1 | Tagged Vlans: NONE

Peer Port Configuration (optional): Device: | Slot.Port: | Port Profile: | MLPPP Instance: NONE | Timing Reference: SELF

Schedule: ● Now ○ Hold ○ Schedule: Jun 7, 2013 7 23 AM

FIGURE 14-7 Provision New NTE-DS1 Port Form

TABLE 14-4 Provision Port for NTE8-DS1/E1Form

Panel	Field/Button	Description
Top of Form	Description (Customer ID)	A way to identify the customer. The name should be descriptive so it can be easily recognized, especially on the Ports table in Network Inventory. The name should be unique to differentiate it from other customers, but in some configurations the name can apply to more than one port, such as DS1/E1 ports for NTE8. Refer to "NTE8 Dual Circuit Provisioning" on page 653.
PPP Configuration	Device	A drop-down of all the devices that have NTE8 cards configured as DS1 ports (or, if the port is an E1, all the devices that have NTE8 cards configured as E1 ports).
	Slot.Port	A drop-down of the ports (card.slot) in the selected device that are DS1 or E1, depending on the port type being configured.

TABLE 14-4 Provision Port for NTE8-DS1/E1Form

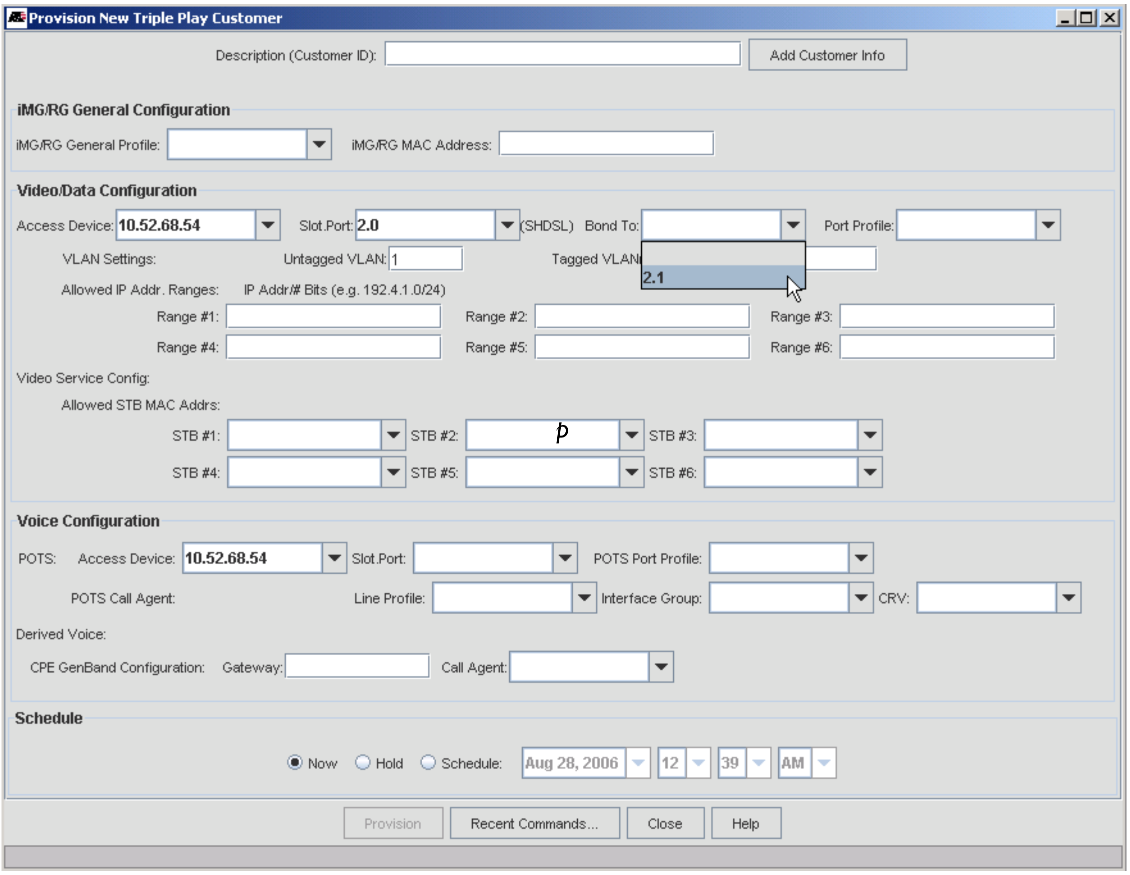
Panel	Field/Button	Description
	Port Profile	The available profiles for the port type (DS1 or E1) appear in the drop-down list. When the port is provisioned, it will inherit the attributes of that profile.
	MLPPP Instance	The MLPPP that the DS1/E1 will be associated with. When more than one DS1/E1 is bundled together, each DS1/E1 is associated with a PPP, and the PPPs are all associated with one MLPPP. The pull-down has three attributes: - The numbering of the MLPPP begins with the slot and an id number starting at 8. - The membership includes the members of the MLPPP and shows Empty if there are no PPPs associated with the MLPPP. - The provisioning status shows whether the MLPPP with this id has already been created. If it has, it shows EXISTS. If not, it shows NEW. If there is only one DS1/E1 to be part of the connection (and therefore only one PPP), there is no MLPPP instance and so NONE should be chosen. *Note: The user can still create an MLPPP instance with only one PPP if desired.*
	Timing Reference	Where the port will get its clocking reference from. The choices are: - SELF - Itself - CARD - The “card-level” timing reference.
PPP Configuration	PPP Parameters	The parameters for the associated PPP. The default values are displayed.
	MLPPP Parameters	The MLPPP parameters. If NONE has been selected for the MLPPP Instance, these fields are blank. If an MLPPP instance is selected, and then a peer port is selected, the MLPPP Instance field in the Peer Port Configuration panel is activated.
	VLAN Parameters	
Peer Port Configuration (optional)	Device	The device that contains the peer DS1/E1 port.
	Port	A drop-down of the ports (card.slot) in the selected device that are DS1 or E1, depending on the port type being configured *Note: A peer port can be on a different device or the same device as the port, but cannot be on the same card.*
	Port Profile	The available profiles for the port type (DS1 or E1) appear in the drop-down list. When the port is provisioned, it will inherit the attributes of that profile.
	MLPPP Instance	The MLPPP instance that the peer DS1/E1 port is associated with.

TABLE 14-4 Provision Port for NTE8-DS1/E1Form

Panel	Field/Button	Description
	Timing Reference	Where the port will get its clocking reference from.
Bottom of Form	Provision	Enabled only after the minimum number of correct fields have been data filled, and these fields have been data filled with valid values.

14.6 Provision New Customer / Port for SHDSL16/24

The following figure shows the Triple Play Customer Form for a SHDSL24 port. Note that you can only choose odd-numbered port for first port if doing bonded.



Provision New Triple Play Customer

Video/Data Configuration

Access Device: 10.52.68.54

Slot.Port: 2.0 (SHDSL)

Bond To: 2.1

Untagged VLAN: 1

Voice Configuration

POTS: Access Device: 10.52.68.54

Schedule

● Now ○ Hold ○ Schedule: Aug 28, 2006 12 39 AM

FIGURE 14-8 Provisioning SHDSL24 Port

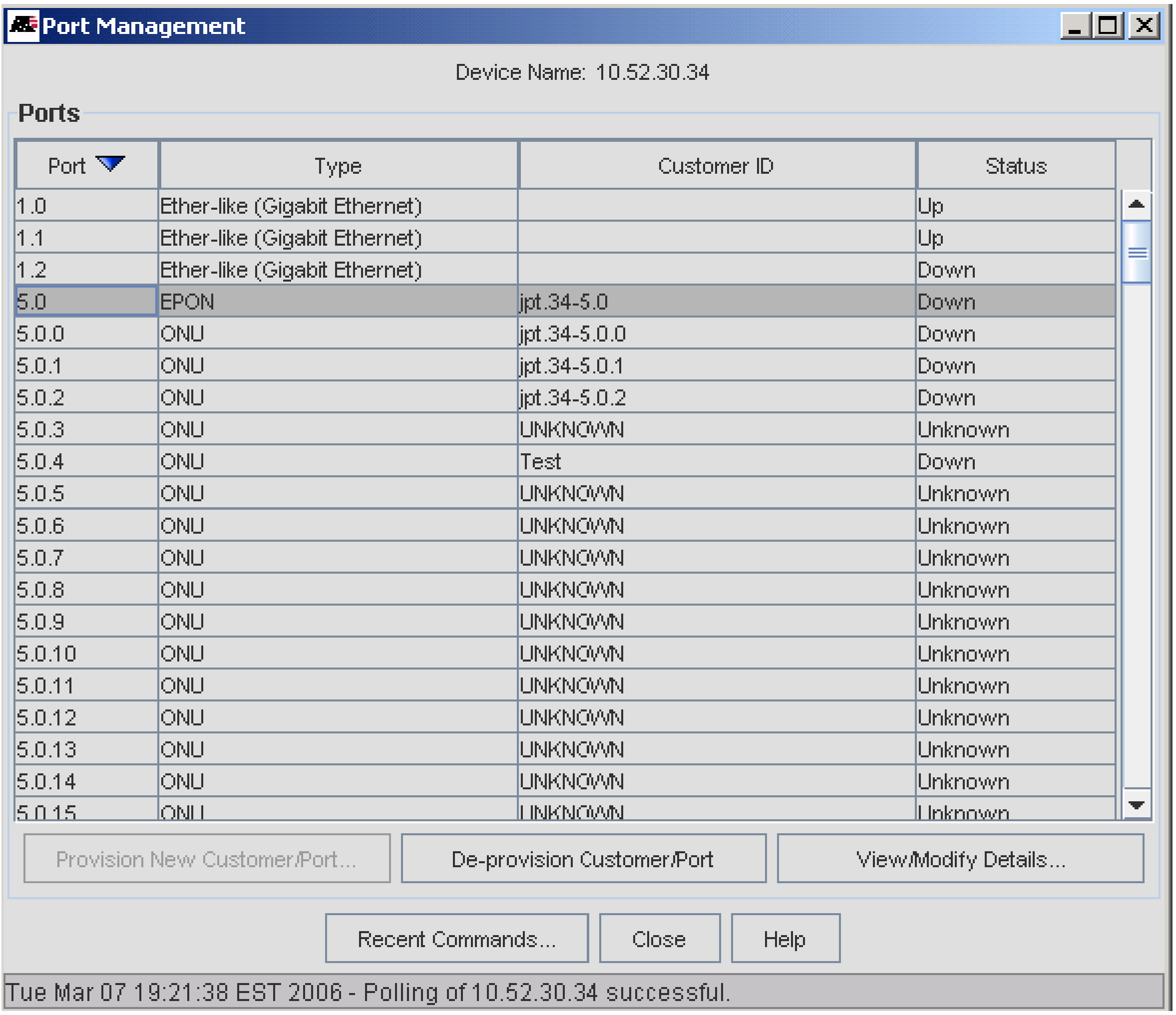
14.7 Provision New EPON Port

The EPON port is part of the configuration that includes the EPON2 card (for passive optical network) and the iMG646PX-ON model which includes the Optical Networking Unit (ONU).

Note: *For complete information about the EPON2 card, ONU, QoS policies being associated with VLANs, etc. refer to the Software Reference for iMAP Series Switches.*

The numbering for the EPON ports is the standard slot.port.

The following figure shows the Port Management Form for a device and how the EPON ports are shown. The EPON2 port is 5.0.



Device Name: 10.52.30.34

Ports

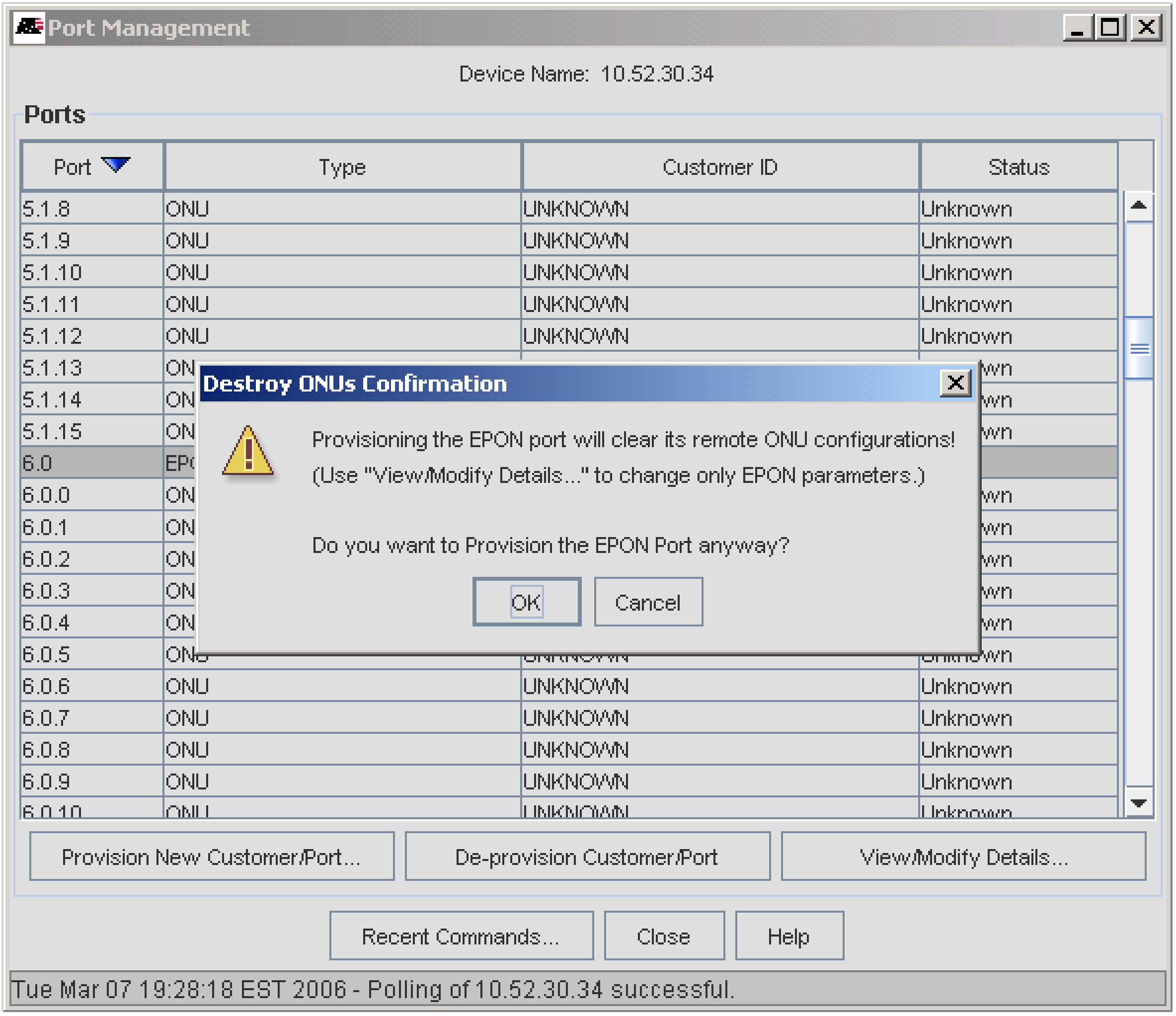
Port	Type	Customer ID	Status
1.0	Ether-like (Gigabit Ethernet)		Up
1.1	Ether-like (Gigabit Ethernet)		Up
1.2	Ether-like (Gigabit Ethernet)		Down
5.0	EPON	jpt.34-5.0	Down
5.0.0	ONU	jpt.34-5.0.0	Down
5.0.1	ONU	jpt.34-5.0.1	Down
5.0.2	ONU	jpt.34-5.0.2	Down
5.0.3	ONU	UNKNOWN	Unknown
5.0.4	ONU	Test	Down
5.0.5	ONU	UNKNOWN	Unknown
5.0.6	ONU	UNKNOWN	Unknown
5.0.7	ONU	UNKNOWN	Unknown
5.0.8	ONU	UNKNOWN	Unknown
5.0.9	ONU	UNKNOWN	Unknown
5.0.10	ONU	UNKNOWN	Unknown
5.0.11	ONU	UNKNOWN	Unknown
5.0.12	ONU	UNKNOWN	Unknown
5.0.13	ONU	UNKNOWN	Unknown
5.0.14	ONU	UNKNOWN	Unknown
5.0.15	ONU	UNKNOWN	Unknown

Tue Mar 07 19:21:38 EST 2006 - Polling of 10.52.30.34 successful.

FIGURE 14-9 Provision EPON Port

To provision on EPON port, the user should select a port that has a status of Unknown with no Customer ID and then select the activated Provision New Customer Port button.

Warning: If the user tries to provision a port with configured ONUs, the ONU configurations are destroyed, as shown in the following figure.



Device Name: 10.52.30.34

Ports

Port	Type	Customer ID	Status
5.1.8	ONU	UNKNOWN	Unknown
5.1.9	ONU	UNKNOWN	Unknown
5.1.10	ONU	UNKNOWN	Unknown
5.1.11	ONU	UNKNOWN	Unknown
5.1.12	ONU	UNKNOWN	Unknown
5.1.13	ON		wn
5.1.14	ON		wn
5.1.15	ON		wn
6.0	EP		
6.0.0	ON		wn
6.0.1	ON		wn
6.0.2	ON		wn
6.0.3	ON		wn
6.0.4	ON		wn
6.0.5	ONU		wn
6.0.6	ONU	UNKNOWN	Unknown
6.0.7	ONU	UNKNOWN	Unknown
6.0.8	ONU	UNKNOWN	Unknown
6.0.9	ONU	UNKNOWN	Unknown
6.0.10	ONU	UNKNOWN	Unknown

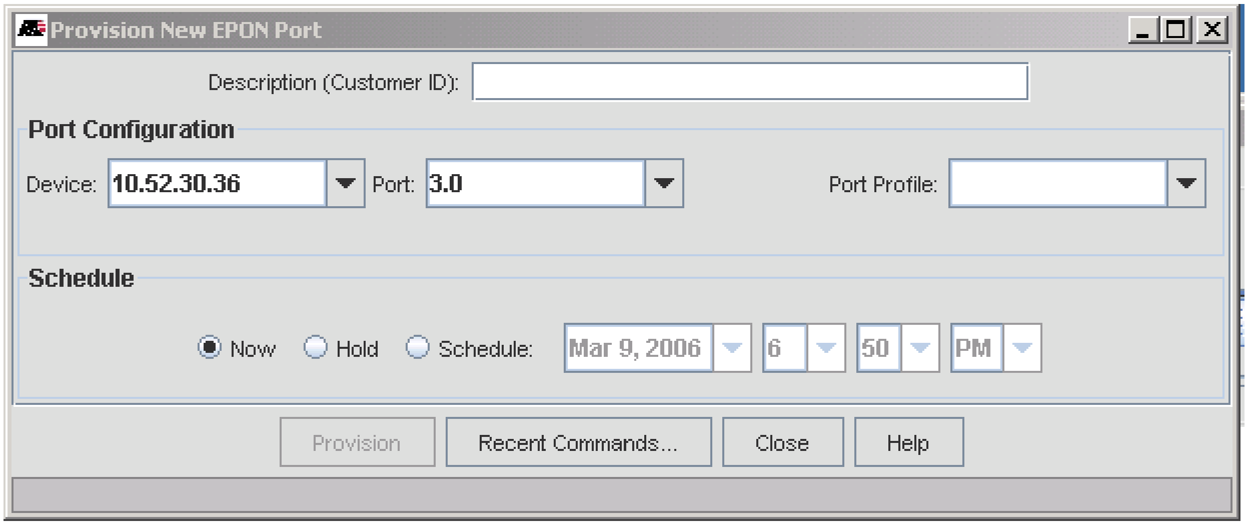
Destroy ONUs Confirmation

Provisioning the EPON port will clear its remote ONU configurations!
(Use "View/Modify Details..." to change only EPON parameters.)

Do you want to Provision the EPON Port anyway?

Tue Mar 07 19:28:18 EST 2006 - Polling of 10.52.30.34 successful.

FIGURE 14-10 Trying to Provision an EPON with Configured ONUs



Description (Customer ID):

Port Configuration

Device: 10.52.30.36 Port: 3.0 Port Profile:

Schedule

● Now ○ Hold ○ Schedule: Mar 9, 2006 6 50 PM

FIGURE 14-11 Provision New EPON Port

14.8 Provision New Customer / Port for ONU

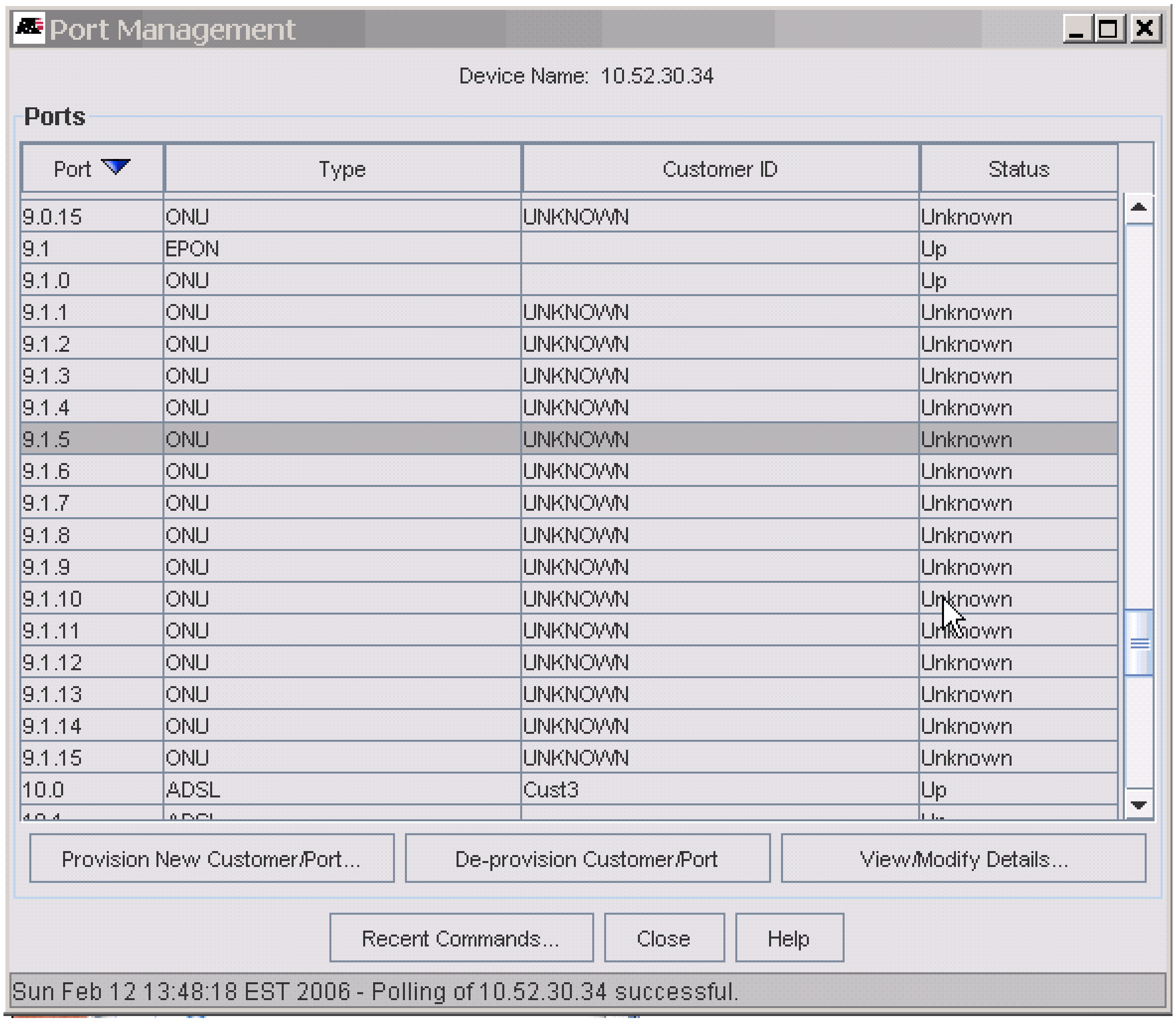
The ONU is part of the configuration that includes the EPON2 card (for passive optical network) and the Optical Networking Unit (ONU).

Note: For complete information about the EPON2 card, ONU, QoS policies being associated with VLANs, etc. refer to the Software Reference for iMAP Series Switches.

From the perspective of the AlliedView NMS, the ONU is considered a customer port regardless of whether it connected to an iMG646PX-ON, ON1000, or other Media Converter, and therefore is included with the other ports on an iMAP device that can be provisioned using the Triple Play Form. The numbering for the ONUs is a three digit port number, the first two being the EPON port interface.

When creating the ONU, the system will query to ONU and datafill the configuration as part of an iMG/RG or ON1000. When the user wishes to change the ONU type, it must be destroyed and then re-created.

The following figure shows the Port Management Form for a device and how the ONU ports are shown. The EPON2 port is 9.1 and so the ONUs are numbered 9.1.0, 9.1.1, etc.



Device Name: 10.52.30.34

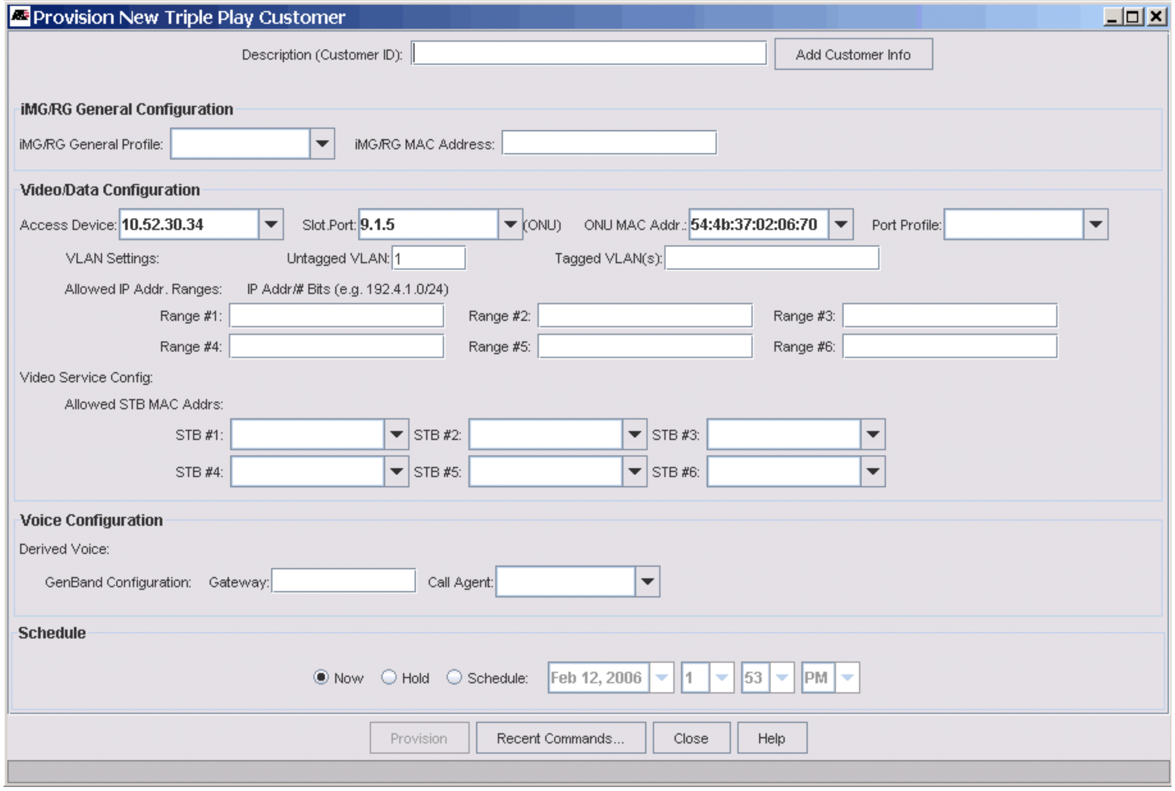
Ports

Port	Type	Customer ID	Status
9.0.15	ONU	UNKNOWN	Unknown
9.1	EPON		Up
9.1.0	ONU		Up
9.1.1	ONU	UNKNOWN	Unknown
9.1.2	ONU	UNKNOWN	Unknown
9.1.3	ONU	UNKNOWN	Unknown
9.1.4	ONU	UNKNOWN	Unknown
9.1.5	ONU	UNKNOWN	Unknown
9.1.6	ONU	UNKNOWN	Unknown
9.1.7	ONU	UNKNOWN	Unknown
9.1.8	ONU	UNKNOWN	Unknown
9.1.9	ONU	UNKNOWN	Unknown
9.1.10	ONU	UNKNOWN	Unknown
9.1.11	ONU	UNKNOWN	Unknown
9.1.12	ONU	UNKNOWN	Unknown
9.1.13	ONU	UNKNOWN	Unknown
9.1.14	ONU	UNKNOWN	Unknown
9.1.15	ONU	UNKNOWN	Unknown
10.0	ADSL	Cust3	Up

Sun Feb 12 13:48:18 EST 2006 - Polling of 10.52.30.34 successful.

FIGURE 14-12 Port Management Form for Device with EPON2/ONU Ports

The user can then select Provision New Customer Port to bring up the Triple Play form, as shown in the following figure.



Access Device: 10.52.30.34

Slot.Port: 9.1.5 (ONU)

ONU MAC Addr.: 54:4b:37:02:06:70

Untagged VLAN: 1

● Now ○ Hold ○ Schedule: Feb 12, 2006 1 53 PM

FIGURE 14-13 Triple Play Form for an ONU Customer Port

Note the following attributes of the Triple Play Form when provisioning an ONU:

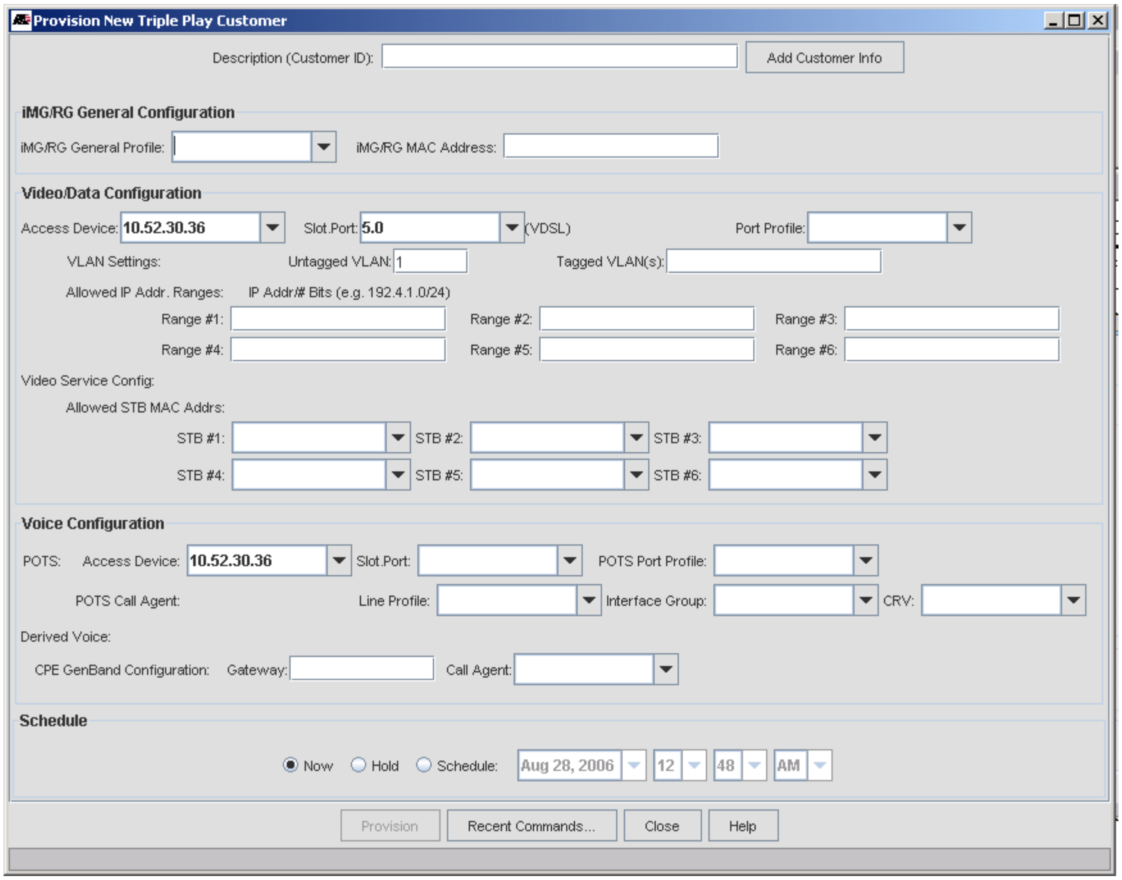
- The Slot.Port has three digits for the ONU.
- The MAC address that has been assigned to the ONU is displayed.

Note: *If the administrator is provisioning an iMG646PX-ON, the iMG/RG General Configuration Panel would be filled in, as shown in Section 7.*

14.9 Provision New Customer / Port for VDSL24A/B

The VDSL card connects to a VDSL modem.

Note: *A VDSL-based iMG/RG is not yet available.*



Provision New Triple Play Customer

Description (Customer ID): Add Customer Info

iMG/RG General Configuration

iMG/RG General Profile: iMG/RG MAC Address:

Video/Data Configuration

Access Device: 10.52.30.36 Slot.Port: 5.0 (VDSL) Port Profile:

VLAN Settings: Untagged VLAN: 1 Tagged VLAN(s):

Allowed IP Addr. Ranges: IP Addr/# Bits (e.g. 192.4.1.0/24)

Range #1: Range #2: Range #3:

Range #4: Range #5: Range #6:

Video Service Config:

Allowed STB MAC Addrs:

STB #1: STB #2: STB #3:

STB #4: STB #5: STB #6:

Voice Configuration

POTS: Access Device: 10.52.30.36 Slot.Port: POTS Port Profile:

POTS Call Agent: Line Profile: Interface Group: CRV:

Derived Voice:

CPE GenBand Configuration: Gateway: Call Agent:

Schedule

● Now ○ Hold ○ Schedule: Aug 28, 2006 12 48 AM

FIGURE 14-14 Provision VDSL Port

Note the following on filling out the Triple-Play form for VDSL:

- The pull-down for the iMG/RG General configuration is left blank.
- The Voice Configuration panel is left blank.

14.10 Overview of Triple Play Service Management Form

Once a port is configured for video, data, or voice, you use the Triple Play Service Management Form to view or modify the port's attributes. Depending on the type of port configured and the services configured on that port, this management form displays the various attributes in a hierarchical multi-tab format. The following sections give the different ways this form can appear:

- Status ("Status Tab" on page 413)
- Add a voice Line (for GenBand only) ("Add Derived Voice Line for GenBand (on Status Tab Form)" on page 414)
- iMG/RG ("iMG/RG Tab" on page 415)
- Ethernet Configuration ("Ether-like Config. Tab" on page 417)
- ADSL Configuration ("ADSL Configuration Tab" on page 426)
- SHDSL Configuration ("SHDSL Port Management Form" on page 444)
- Voice Configuration ("Voice Port Management (Tabbed Form)" on page 448)
- CES8 ("CES8 Port (DS1/E1 Port Management Tabbed Form)" on page 456)
- NTE8 ("NTE8 Port Management Form" on page 463)

- EPON2/ONU ("ONU Configuration (as ON1000 or as part of iMG646PX-ON)" on page 476)
- ATM Bonding ("ATM Bonding" on page 487)

The iMG/RG is included in the Customer Management Form. Note that once the iMG/RG is provisioned with the iMAP customer port, this form displays the same information whether viewing the RG device or the iMAP interfacing port.

In provisioning Triple Play, more than one card can be included in the customer configuration, and so a combination of tabs will appear so the user can query all attributes of the customer.

This section includes an overview of what the tabs include for the iMG/RG, but focuses on ports that are not configured with an iMG/RG.

14.11 Status Tab

The Status tab gives the main provisioning attributes for the port/RG and their status. It also allows the administrator to add a voice line, as detailed in "Add Derived Voice Line for GenBand (on Status Tab Form)" on page 414. The following figure shows an example form and its attributes.

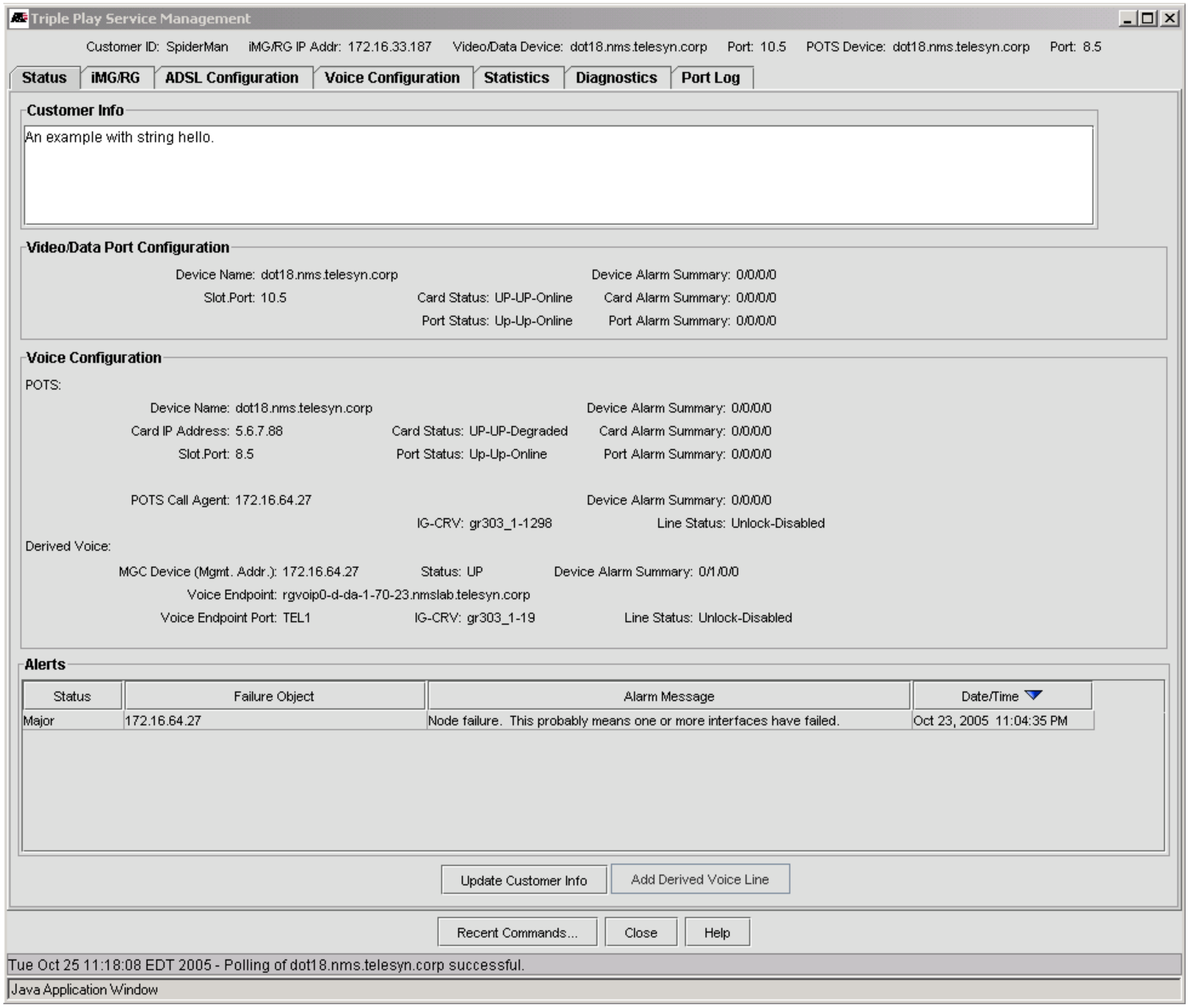
The status form allows the user to see in one set of screens the attributes that were used when provisioning the iMG (use of profiles, VLANs, etc.) as well as the status of the iMG.

For voice service, there are two sets of information under the Voice configuration panel:

- **POTS** - When configured, this is voice service using a POTS-based card (POTS24, PAC24) and an ADSL splitter. This includes the slot.port of the POTS24 card, the call agent, and the status of the POTS24 card and port. If there is no POTS configured, there is the text “No POTS port configured.”

Note: If the POTS24 configuration uses a soft switch other than GenBand, the POTS call agent attributes are listed as unknown.

- **Derived Voice** - When configured, this is VoIP provided by the iMG/RG/iBG and can use one of many softswitches, including GenBand. If the configuration uses GenBand, then the Derived Voice attributes are shown, including the Voice Endpoint, which must be configured for this voice service to work. If another softswitch is used, there is the message “Derived voice gateway information is not available.” This means that the NMS does not manage the device that provides the service.



Customer ID: SpiderMan iMG/RG IP Addr: 172.16.33.187 Video/Data Device: dot18.nms.telesyn.corp Port: 10.5 POTS Device: dot18.nms.telesyn.corp Port: 8.5

Customer Info

An example with string hello.

Video/Data Port Configuration

Device Name: dot18.nms.telesyn.corp
Device Alarm Summary: 0/0/0/0
Slot.Port: 10.5
Card Status: UP-UP-Online
Card Alarm Summary: 0/0/0/0
Port Status: Up-Up-Online
Port Alarm Summary: 0/0/0/0

Voice Configuration

POTS:

Device Name: dot18.nms.telesyn.corp
Device Alarm Summary: 0/0/0/0
Card IP Address: 5.6.7.88
Card Status: UP-UP-Degraded
Card Alarm Summary: 0/0/0/0
Slot.Port: 8.5
Port Status: Up-Up-Online
Port Alarm Summary: 0/0/0/0

POTS Call Agent: 172.16.64.27
Device Alarm Summary: 0/0/0/0
IG-CRV: gr303_1-1298
Line Status: Unlock-Disabled

Derived Voice:

MGC Device (Mgmt. Addr.): 172.16.64.27
Status: UP
Device Alarm Summary: 0/1/0/0
Voice Endpoint: rgvoip0-d-da-1-70-23.nmslab.telesyn.corp
Voice Endpoint Port: TEL1
IG-CRV: gr303_1-19
Line Status: Unlock-Disabled

Alerts

Status	Failure Object	Alarm Message	Date/Time ▼
Major	172.16.64.27	Node failure. This probably means one or more interfaces have failed.	Oct 23, 2005 11:04:35 PM

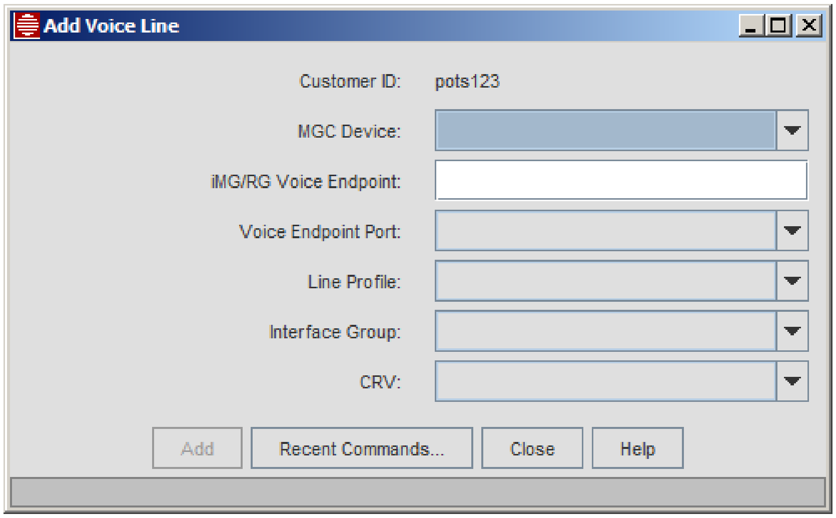
Tue Oct 25 11:18:08 EDT 2005 - Polling of dot18.nms.telesyn.corp successful.

Java Application Window

FIGURE 14-15 Example Status Form (POTS24 and Derived Voice using GenBand)

14.12 Add Derived Voice Line for GenBand (on Status Tab Form)

When the GenBand configuration is being used, the administrator can add a voice line immediately on the Status form by clicking **Add Genband Derived Voice Line**. The following form appears:



Customer ID:	pots123
MGC Device:	
iMG/RG Voice Endpoint:	
Voice Endpoint Port:	
Line Profile:	
Interface Group:	
CRV:	

FIGURE 14-16 Add Voice Line Form

If a voice line has already been configured, the MGCP Device and iMG/RG Voice Endpoint (DNS name) are already provided, and the pull-downs should be filled in descending order, since one will drive what is available in the next pull-down. After choosing **Add**, you should see an additional MGCP Line Info tab in the Voice Configuration form. The corresponding line in the Voice Service tab in the iMG/RG form must then be enabled (by clicking the Enabled check box for the New Line Configuration).

If a voice line is being added for the first time, the available devices appear in the MGC Device pull-down. Once a device is chosen, the user must input the MAC address of the iMG as well as the attributes from the remaining pull downs.

Note: *This form is only used when the GenBand is providing the derived voice. The NMS does not support GenBand provisioning with TR-008.*

14.13 iMG/RG Tab

This form lists all the major attributes of the iMG/RG and its services, and includes the attributes that were filled out as part of the iMG/RG profiles.

Note: *At the bottom of the form are two buttons, Modify and Save iMG/RG Configuration. After changing any fields in any tabbed forms in the iMG/RG form, the user should click Modify, wait until finished, and then Save iMG/RG Configuration. This ensures the changes take effect immediately and after an iMG/RG reboot.*

14.13.1 Mgmt. Info Tab

This form includes the iMG/RG Type and the iMG/RG General Profile that is associated with the iMG/RG. From this form, the user can change the associated RG General Profile (Mgmt. Info tab) as well as specific attributes that do not match what was in the Profile. Refer to "iMG General Profile" on page 702 for a description of these fields.

Note: *The user should not change individual fields since they would no longer match those of the associated General Profile. If they are changed, an asterisk (*) appears next to the General Profile Name.*

14.13.2 Wireless Tab

For the iMG/RG wireless devices (as well as Comtrend, starting in release 11.0 SP3), the wireless tab includes the parameters that are relevant for the wireless configuration. For certain devices, the subscriber has the ability to change these parameters. Refer to "Split Management for Wireless iMGs" on page 812.

14.13.3 Port Assignments Tab

This form shows the Port assignments that were data filled in the associated RG General Profile (Port Assignment tab). The user selects a port in the New Port Assignment Panel and selects the different attributes from the pull-downs.

Note: The user should not change individual fields since they would no longer match those of the associated General Profile.

14.13.4 IP Routes Tab

This form shows the IP Route assignments that were data filled in the associated RG General Profile (IP Routes tab). The user selects a route in the New IP Routes Panel, selects or deselects the Enable tic box, and then selects the different attributes from the pull-downs.

Note: The user should not change individual fields since they would no longer match those of the associated General Profile.

14.13.5 Internet Service Tabs

These forms show the Internet Service attributes that were data filled in the associated Internet Service Profile. From these forms, the user can change the associated Internet Service Profile as well as specific attributes that do not match what was in the Profile. Refer to "iMG Internet Profile" on page 713 for a description of these fields. If you change individual fields on this form note they will no longer match the associated profile.

The tabs that appear are:

- Internet Service
- Security
- Firewall
- NAT

14.13.6 Video Service Tab

This form shows the Video Service attributes that were data filled in the associated Video Service Profile. From this form, the user can change the associated Video Service Profile as well as specific attributes that do not match what was in the Profile. Refer to "iMG Video Profile" on page 727 for a description of these fields. If you change individual fields on this form note they will no longer match the associated profile.

14.13.7 Voice Service Tab

This form shows the Voice Service attributes that were entered in the associated Voice Service profile. From this form, you can change the associated Voice Service profile as well as specific attributes that do not match what was in the profile. Refer to "iMG Voice Profile" on page 730 for a description of these fields. If you change individual fields on this form note they will no longer match the associated profile.

Voice Line Registration Name

You can include a registration name for each phone line on devices that use SIP for voice service. To add a voice line registration name:

1. In the **Network Objects** panel, go to **Network Inventory** > **iMG/RGs**
2. In the **iMG/RGs** panel, double-click the device on which you want to add registration names for the voice lines.
3. Select the **iMG/RG** tab, then select the **Voice Service** tab.
4. Under **New Line Configuration**, select the line you want to add a registration name to. If it is not already enabled, check **Enabled**.
5. If you are adding a new line, double-click the cell in the **Number** column and enter the phone number. A voice line cannot have a registration name without a phone number associated with it.

6. Double-click the cell in the **Registration Name** column. Enter the registration name you want to use for the line. You can use a combination of numbers, alphabetic characters, and the hyphen (-), underscore (_) and plus (+) characters. Other special characters and spaces are not allowed.
7. Click **Modify** to save the changes to the line.

14.13.8 Diagnostic Tab for iMG6x6MOD/iMG7x6MOD

In the MOD iMGs, the LAN diagnostic feature was added in release 3.7. The NMS supports this LAN diagnostic functionality. Refer to "iMG LAN Diagnostics" on page 894.

14.14 Ether-like Config. Tab

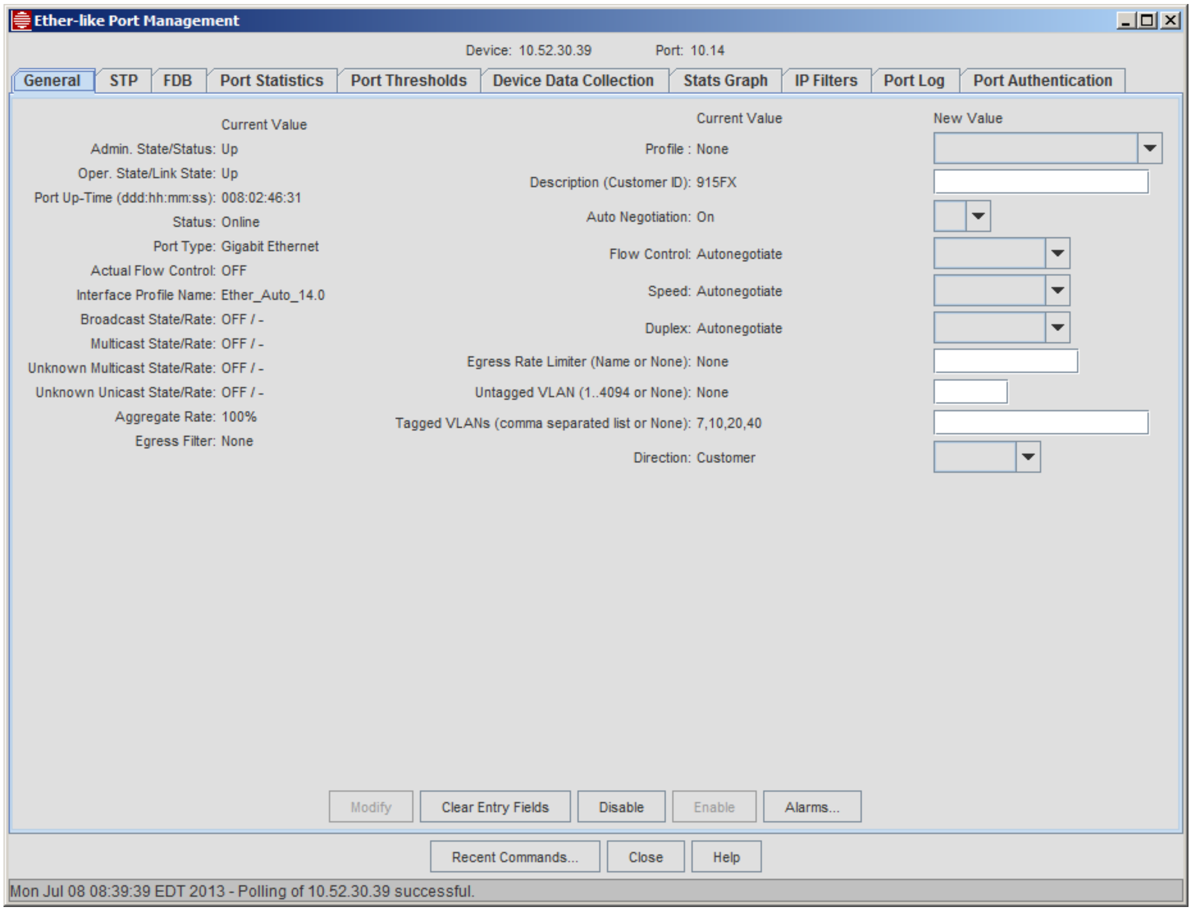
Following are the types of ether-like ports that can be provisioined.

- See “Ether-Like Port (General Tab)” on page 417.
- See “Ether-Like Port (General Tab) - iMG/RG” on page 420.
- See “Ether-Like Port (Port Statistics Tab)” on page 421.
- See “Ether-Like Port (Port Thresholds Tab)” on page 422.
- See “Ether-Like Port (Device Data Collection Tab)” on page 423.
- See “Ether-Like Port (Stats Graph Tab)” on page 423.
- See “Ether-Like Port (IP Filters Tab)” on page 425.
- See “Ether-Like Port (Port Log Tab)” on page 426.
- See “Ether-Like Port (DS3-SFP Tab)” on page 426.
- See “Ether-Like Port (POE Tab)” on page 426.

14.14.1 Ether-Like Port (General Tab)

When a port is labeled Ether-like, then it is an ethernet port facing the network or a customer port facing and customer device, such as an iMG/RG. The following subsections go through these provisioning screens, starting with the General tab.

Note: For the SBx3100, there is an additional tab for PoE for the GE24POE card. Refer to "Ether-Like Port (POE Tab)" on page 426.



Device: 10.52.30.39 Port: 10.14

	Current Value
Admin. State/Status:	Up
Oper. State/Link State:	Up
Port Up-Time (ddd:hh:mm:ss):	008:02:46:31
Status:	Online
Port Type:	Gigabit Ethernet
Actual Flow Control:	OFF
Interface Profile Name:	Ether_Auto_14.0
Broadcast State/Rate:	OFF / -
Multicast State/Rate:	OFF / -
Unknown Multicast State/Rate:	OFF / -
Unknown Unicast State/Rate:	OFF / -
Aggregate Rate:	100%
Egress Filter:	None

	Current Value	New Value
Profile :	None	
Description (Customer ID):	915FX	
Auto Negotiation:	On	
Flow Control:	Autonegotiate	
Speed:	Autonegotiate	
Duplex:	Autonegotiate	
Egress Rate Limiter (Name or None):	None	
Untagged VLAN (1..4094 or None):	None	
Tagged VLANs (comma separated list or None):	7,10,20,40	
Direction:	Customer	

Mon Jul 08 08:39:39 EDT 2013 - Polling of 10.52.30.39 successful.

FIGURE 14-17 Ether like Port Management Window - General

TABLE 14-5 Ether-like Port Management for iMAP Devices - General Tab

Field/Button	Description
Admin. State/Status	The Administrative State can be controlled and determines the Operational State.
Oper. State/Link State	The ability of the port to provide service. The Administrative State must be up and then the system determines if the port can provide service.
Port Up-Time	Amount of time the physical interface has been in the UP-UP-Online state.
Status	The status of the port that follows form the Administrative State and Operational State. For meanings, refer to the *Software Reference for iMAP Series Switches*. - ONLINE - IN TEST - FAILED - OFFLINE - DEPENDENCY - DEGRADED - NOT INSTALLED - INITIALIZATION REQUIRED - TERMINATING
Port Type	For these Ethernet ports, Optical Fast Ethernet

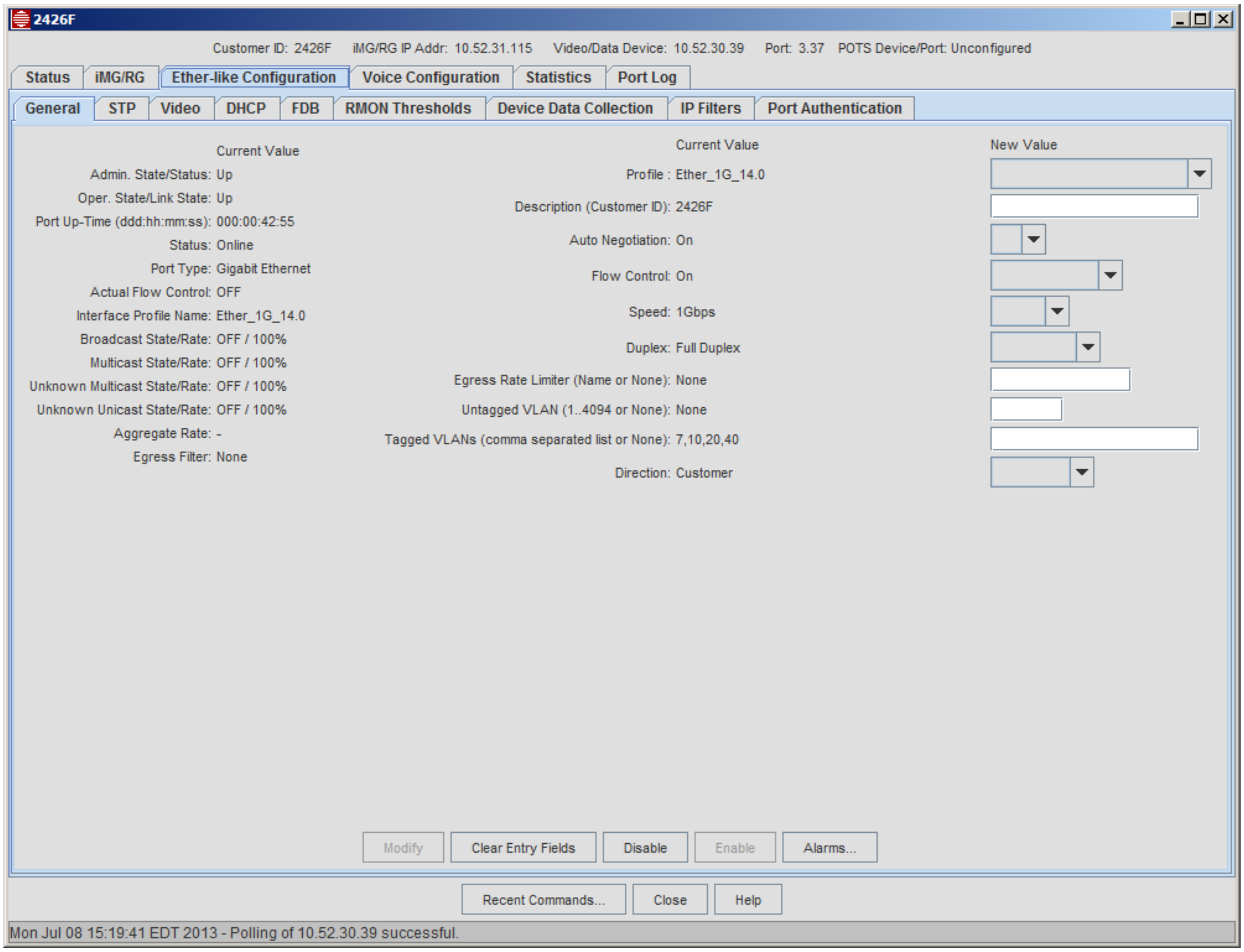
TABLE 14-5 Ether-like Port Management for iMAP Devices - General Tab

Field/Button	Description
Actual Flow Control	Whether flow control is on, regardless of how it was provisioned.
Interface Profile Name	The initial port profile name when the port was provisioned.
Broadcast State/Rate	Whether storm control is enabled for broadcast traffic and the rate associated with it. See Configuring Storm Control.
Multicast State/Rate	Whether storm control is enabled for both known and unknown multicast traffic and the rate associated with it. See Configuring Storm Control.
Unknown Multicast State/ Rate	Whether storm control is enabled for unknown multicast traffic only and the rate associated with it. See Configuring Storm Control.
Unknown Unicast State/Rate	Whether storm control is enabled for unknown unicast traffic and the rate associated with it. See Configuring Storm Control.
Aggregate Rate	The percentage (rate) of operational bandwidth of the interfaces that will be usable by all traffic types that have storm control enabled. See Configuring Storm Control.
Egress Filter	Whether egress traffic filtering is enabled. Options are as follows: - None - Broadcast - Unknown Unicast - All See Configuring Storm Control.
Profile	The port profile that is applied to the device.
Description (Customer ID)	An ID that can be given to uniquely identify the port.
Auto Negotiation	Whether certain port attributes are auto-negotiated with the remote peer.
Flow Control	The provisioned flow control.
Speed	The configured port speed.
Duplex	The configured duplex mode.
Actual Port Speed	The measured port speed versus what was actually configured.
Actual Duplex Mode	The duplex mode actually attained.
Egress Rate Limiter	Whether egress rate limiting has been applied.
Untagged VLAN	The VLAN that is applied if the packet has no VLAN id.
Tagged VLANs	The VLANs that are allowed on the port (packet has one of the VLAN IDs).
Direction	Whether the interface is towards the network or customer.
Modify	Enables the any changes have been made to the settings, makes them
Clear Entry Fields	Clears the writable fields of any values.
Disable	Disable the port (after a confirmation window). This makes the overall state DOWN.
Enable	Enable the port. This makes the overall state UP if the port can be brought into service.
Alarms	Brings up the Alarm view for the selected port.
Recent Commands	Views the CLI commands and responses for the operations performed in the Port Management application. This is the same for all tabs.
Close	Closes the View Details application (the window as well as the tab). This is the same for all tabs.

Note: *The Autonegotiation, Flow Control, Speed, and Duplex Mode fields appear according to the port type. (FX has Flow Control, GE has Autonegotiate and Flow Control, FE has Flow Control, Speed and Duplex Mode.*

14.14.2 Ether-Like Port (General Tab) - iMG/RG

When the Ethernet port interfaces with an iMG/RG, there are additional fields that appear. Refer to the following figure.



Customer ID: 2426F iMG/RG IP Addr: 10.52.31.115 Video/Data Device: 10.52.30.39 Port: 3.37 POTS Device/Port: Unconfigured

Current Value

Admin. State/Status: Up
Oper. State/Link State: Up
Port Up-Time (ddd:hh:mm:ss): 000:00:42:55
Status: Online
Port Type: Gigabit Ethernet
Actual Flow Control: OFF
Interface Profile Name: Ether_1G_14.0
Broadcast State/Rate: OFF / 100%
Multicast State/Rate: OFF / 100%
Unknown Multicast State/Rate: OFF / 100%
Unknown Unicast State/Rate: OFF / 100%
Aggregate Rate: -
Egress Filter: None

Current Value New Value

Profile : Ether_1G_14.0
Description (Customer ID): 2426F
Auto Negotiation: On
Flow Control: On
Speed: 1Gbps
Duplex: Full Duplex
Egress Rate Limiter (Name or None): None
Untagged VLAN (1..4094 or None): None
Tagged VLANs (comma separated list or None): 7,10,20,40
Direction: Customer

Mon Jul 08 15:19:41 EDT 2013 - Polling of 10.52.30.39 successful.

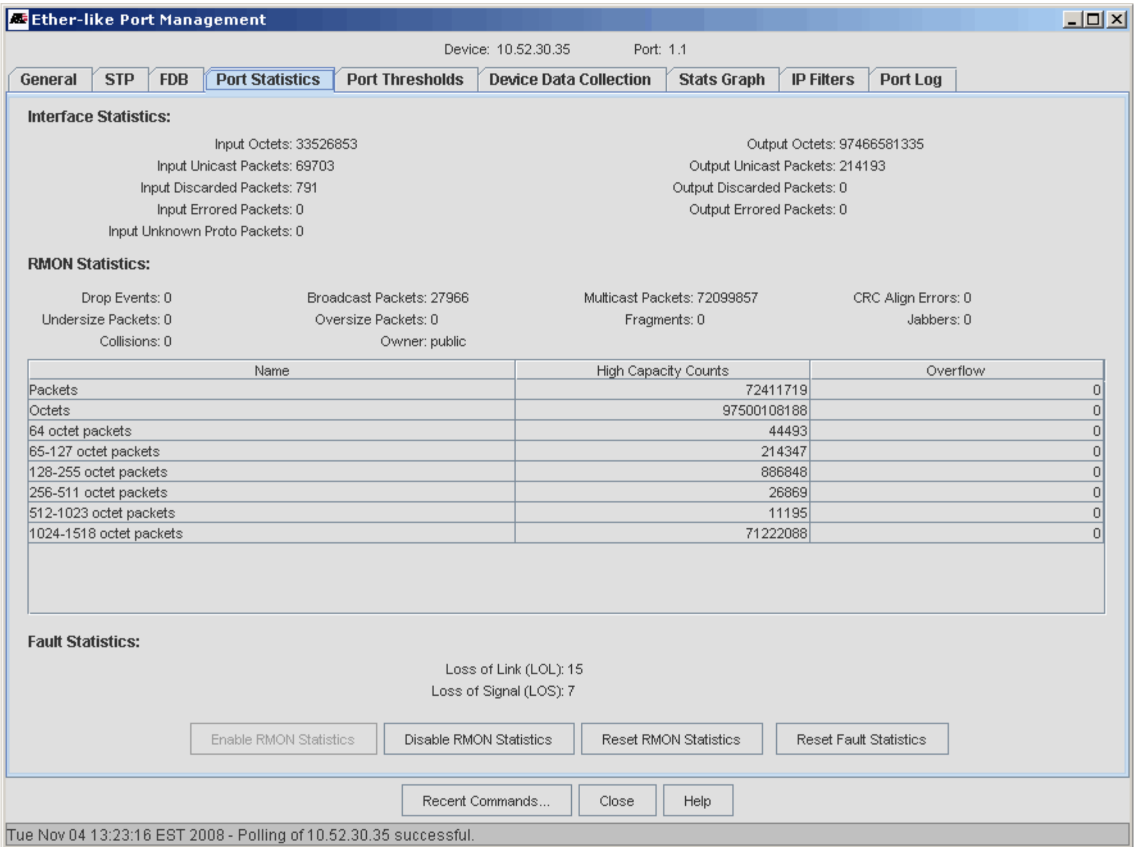
FIGURE 14-18 Ether-like Port Management Window - iMG/RG

Many of the values for the iMG-specific fields are controlled by the profile being used. See "iMG Profiles" on page 701. Note the following fields in particular:

- Multicast MAC Addresses (Video Tab)
- STB MAC Addresses (Video Tab) - MAC addresses for each STB. Addresses can be typed in, selected from the pull-down, or removed (with selection Remove from pull-down).
- Enabled DHCP Relay Instances (DHCP tab) - These are the DHCP instances that are used that allow the RG to boot up and be provisioned correctly. Ensure that all the relevant DHCP instances are enabled. Refer to "Configuring Components for DHCP Discovery" on page 765.

For the tab form descriptions, refer to the ADSL Configuration tab, "ADSL Configuration Tab" on page 426.

14.14.3 Ether-Like Port (Port Statistics Tab)



Ether-like Port Management

Device: 10.52.30.35 Port: 1.1

Interface Statistics:

Input Octets: 33526853
Input Unicast Packets: 69703
Input Discarded Packets: 791
Input Errored Packets: 0
Input Unknown Proto Packets: 0

Output Octets: 97466581335
Output Unicast Packets: 214193
Output Discarded Packets: 0
Output Errored Packets: 0

RMON Statistics:

Drop Events: 0
Undersize Packets: 0
Collisions: 0
Broadcast Packets: 27966
Oversize Packets: 0
Owner: public
Multicast Packets: 72099857
Fragments: 0
CRC Align Errors: 0
Jabbers: 0

Name	High Capacity Counts	Overflow
Packets	72411719	0
Octets	97500108188	0
64 octet packets	44493	0
65-127 octet packets	214347	0
128-255 octet packets	886848	0
256-511 octet packets	26869	0
512-1023 octet packets	11195	0
1024-1518 octet packets	71222088	0

Fault Statistics:

Loss of Link (LOL): 15
Loss of Signal (LOS): 7

Tue Nov 04 13:23:16 EST 2008 - Polling of 10.52.30.35 successful.

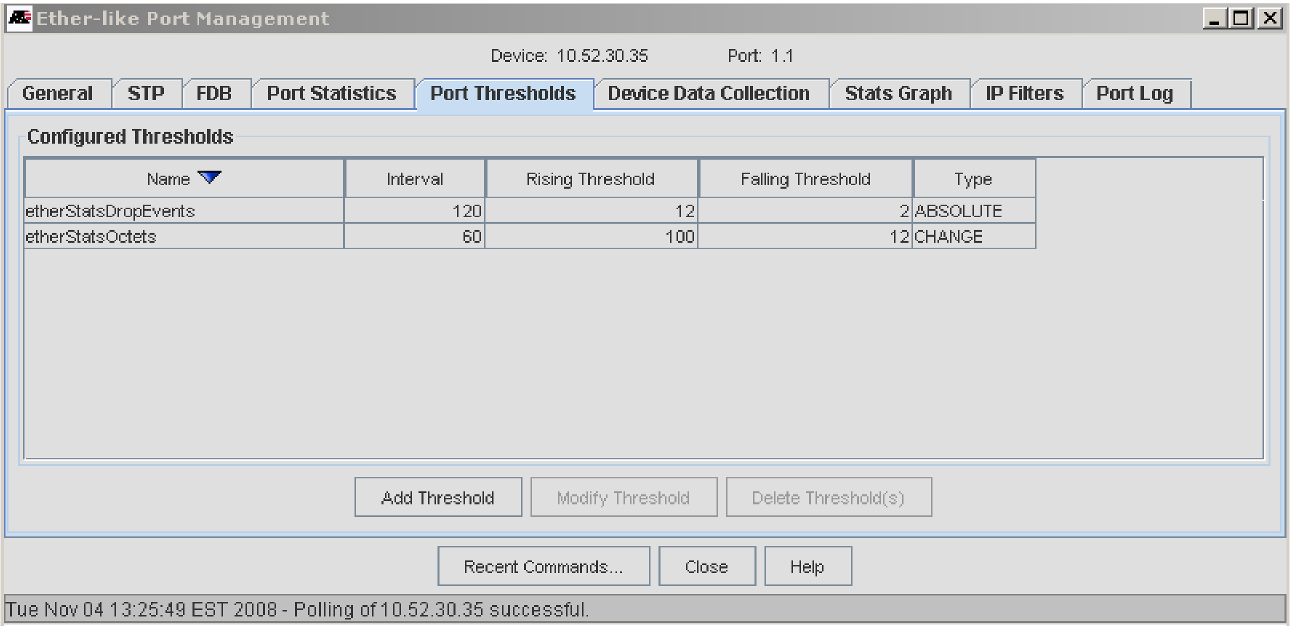
FIGURE 14-19 Ether like Port Management Window - Port Statistics Tab

TABLE 14-6 Provision Port Form for Port Management - Port Statistics Tab

Field/Button	Description
RMON Statistics:	Lists the standard RMON statistics. For an explanation, refer to the *Software Reference for iMAP Series Switches*.
Interface Statistics:	Lists the standard faults for an ethernet port. For an explanation of what these mean and what actions to take (if any), refer to the iMAP Log / Troubleshooting Manual.
Enable Statistics	If the port is UP, this button starts the collection of both RMON and Fault statistics.
Disable Statistics	Discontinues the collection of both RMON and Fault statistics.
Reset Fault Statistics	Resets to 0 the Fault Statistics
Reset RMON Statistics	Resets to 0 the RMON statistics
Command History	Views the CLI commands and responses for the operations performed in the Port Management application. This is the same for all tabs.
Close	Closes the View Details application (the window as well as the tab). This is the same for all tabs.

14.14.4 Ether-Like Port (Port Thresholds Tab)

When an RMON statistic is configured, the attributes determine the interval the statistic will be taken and at what threshold (rising and falling) a log/alarm will be produced. The Port Thresholds tab lists these for the statistics chosen. Form this form statistics can be added, modified, or deleted. Refer to the following figure and table.



Device: 10.52.30.35 Port: 1.1

Name	Interval	Rising Threshold	Falling Threshold	Type
etherStatsDropEvents	120	12	2	ABSOLUTE
etherStatsOctets	60	100	12	CHANGE

Tue Nov 04 13:25:49 EST 2008 - Polling of 10.52.30.35 successful.

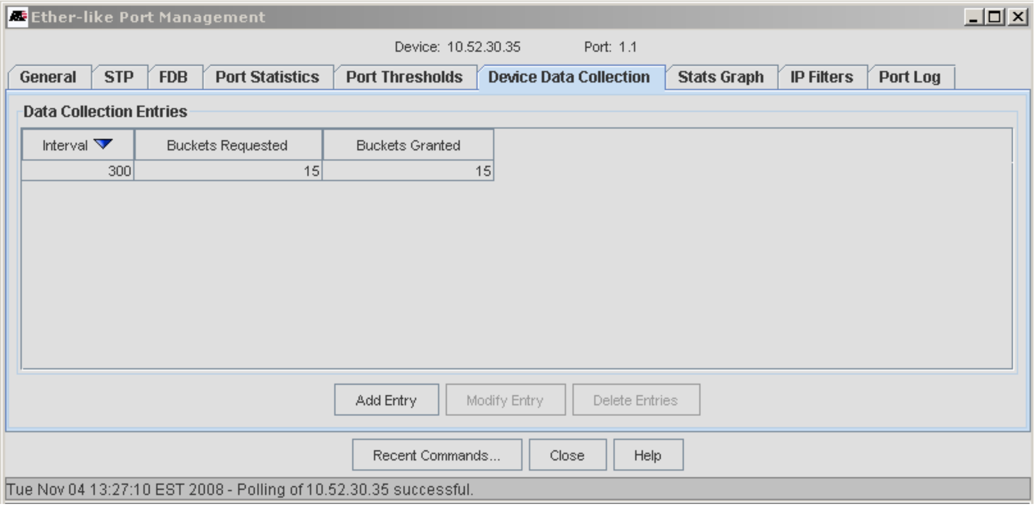
FIGURE 14-20 Ether like Port Management Window - Port Thresholds Tab

TABLE 14-7 Provision Port Form for Port Management - Port Thresholds Tab

Field/Button	Description
Name	One of the RMON statistics
Interval	Interval in number of seconds, from 2 to 3600 (one hour)
Rising Threshold	The number at which an alarm/log is raised when the number is exceeded.
Falling Threshold	The number at which an alarm/log is raised when the number falls above this number. Note that only when this threshold is crossed can another Rising Threshold alarm be raised when the number crosses the Rising Threshold.
Type	The type of threshold to be defined: - ABSOLUTE - The statistic must be reset before the threshold can be crossed again and a log produced. - CHANGE - The logs for thresholds are produced multiple times as the thresholds are crossed. (See Falling Threshold above to understand how this works.)
Add Threshold	Bring up the Add RMON Threshold to Port Form. The fields match what will be displayed.
Modify Threshold	Modify the values for an already created threshold.
Command History	Views the CLI commands and responses for the operations performed in the Port Management application. This is the same for all tabs.
Close	Closes the View Details application (the window as well as the tab). This is the same for all tabs.

14.14.5 Ether-Like Port (Device Data Collection Tab)

The history of statistical data is collected what are called buckets, which collect a certain amount of data over a specific time. By recording and then observing these buckets, users can spot trends. This form is used to define the buckets and their attributes. Refer to the following table and graph.



Device: 10.52.30.35 Port: 1.1

Interval	Buckets Requested	Buckets Granted
300	15	15

Tue Nov 04 13:27:10 EST 2008 - Polling of 10.52.30.35 successful.

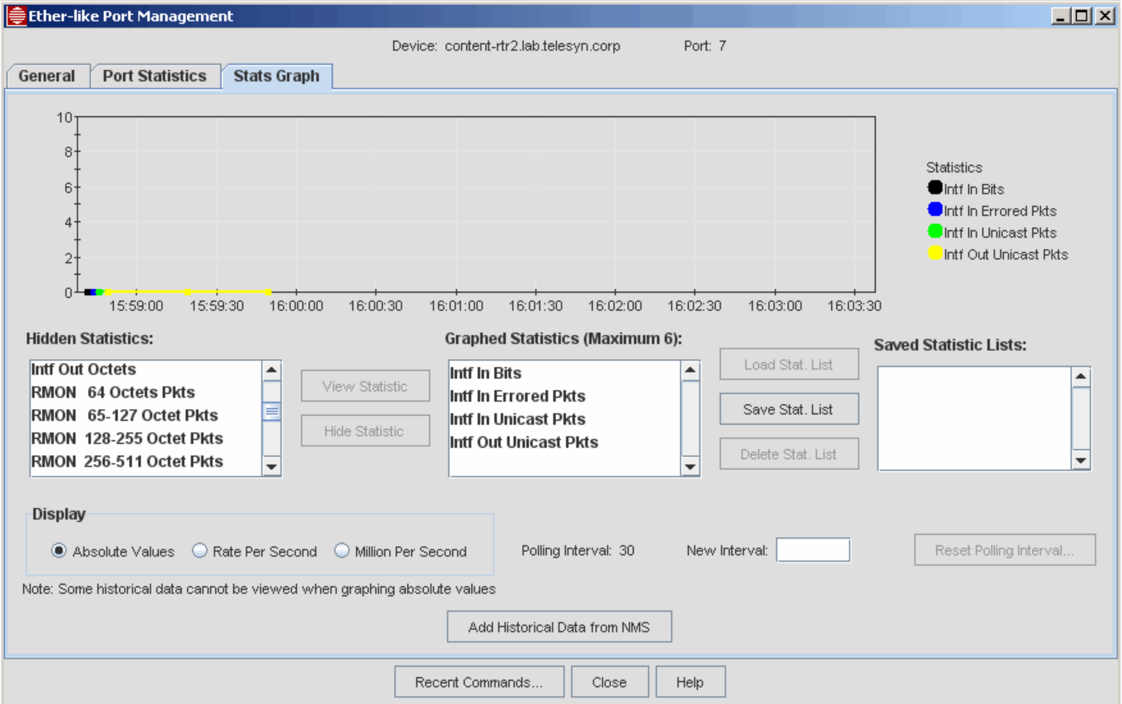
FIGURE 14-21 Ether like Port Management Window - Device Data Collection Tab

TABLE 14-8 Provision Port Form for Port Management - Device Data Collection Tab

Field/Button	Description
Interval	The period of time in seconds statistics will be gathered for a bucket, from 2 to 3600 (one hour)
Buckets Requested	The number of buckets that will be filled before the first bucket is overwritten, from 1 to 2700.
Buckets Granted	The actual number of buckets the device allows.
Valid	Whether the interval and bucket combination are valid. If they are, the column is **Valid.**
Add Entry	Add an interval and bucket combination row.
Modify Entry	Modify a selected interval and bucket combination row.
Delete Entries	Delete the selected entries.
Command History	Views the CLI commands and responses for the operations performed in the Port Management application.
Close	Closes the View Details application (the window as well as the tab).

14.14.6 Ether-Like Port (Stats Graph Tab)

This window makes a graph of selected statistics and displays them with varying attributes.Refer to the following figure and table.



Device: content-rtr2.lab.telesyn.corp Port: 7

Hidden Statistics:

- Intf Out Octets
- RMON 64 Octets Pkts
- RMON 65-127 Octet Pkts
- RMON 128-255 Octet Pkts
- RMON 256-511 Octet Pkts

Graphed Statistics (Maximum 6):

- Intf In Bits
- Intf In Errored Pkts
- Intf In Unicast Pkts
- Intf Out Unicast Pkts

Saved Statistic Lists:

Display

● Absolute Values ○ Rate Per Second ○ Million Per Second

Polling Interval: 30 New Interval:

Note: Some historical data cannot be viewed when graphing absolute values

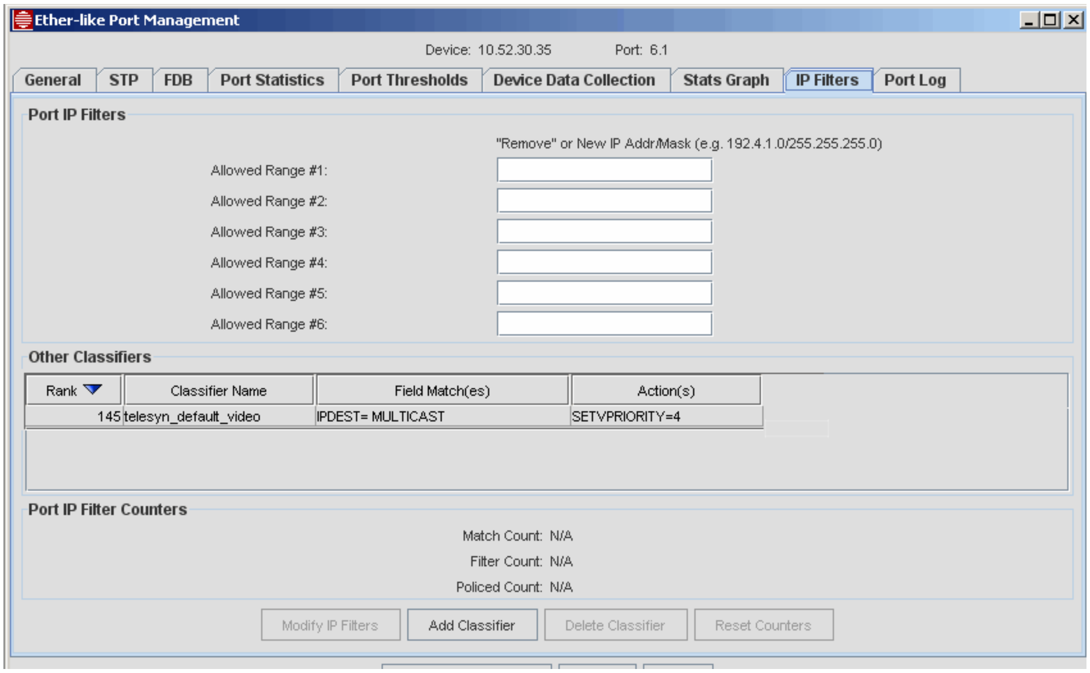
FIGURE 14-22 Ether like Port Management Window - Stats Graph Tab

TABLE 14-9 Provision Port Form for Port Management - Stats Graph Tab

Field/Button	Description
Hidden Statistics:	Statistics not added to the resulting graph
View Statistic:	Enabled when a statistic is chosen form Hidden Statistics, clicking this button adds it to the graph/
Hide Statistic:	Enabled when a statistic is chosen form Graphed Statistics, clicking this button deletes it from the graph/
Display	The attribute that controls the display: - Absolute Values - Rate Per Second - Million Per Second
Polling Interval:	Current Polling Interval in seconds
New Interval:	Sets a new interval for polling. This is set with the **Reset Polling Interval** button.
Enable Statistics	Enables the graph for the statistics chosen.
Disable Statistics:	Disables the graph
Add Historical Data from NMS:	Adds the data collected previously from NMS port management
Add Historical Data from Device:	Adds the data collected previously (buckets) from the device
Command History	Views the CLI commands and responses for the operations performed in the Port Management application. This is the same for all tabs.
Close	Closes the View Details application (the window as well as the tab). This is the same for all tabs.

14.14.7 Ether-Like Port (IP Filters Tab)

For traffic management, the iMAP devices allow the user to control a set of filters on ports, with each classifier given a rank or precedence (the lower the number, the higher the precedence). This form allows the user to list the classifiers that have already been defined and to control the precedence. Refer to the following figure and table.



Device: 10.52.30.35 Port: 6.1

Port IP Filters

"Remove" or New IP Addr/Mask (e.g. 192.4.1.0/255.255.255.0)

Allowed Range #1:

Allowed Range #2:

Allowed Range #3:

Allowed Range #4:

Allowed Range #5:

Allowed Range #6:

Other Classifiers

Rank ▼	Classifier Name	Field Match(es)	Action(s)
145	telesyn_default_video	IPDEST= MULTICAST	SETVPRIORITY=4

Port IP Filter Counters

Match Count: N/A

Filter Count: N/A

Policed Count: N/A

FIGURE 14-23 Ether like Port Management Window - IP Filters Tab

TABLE 14-10 Provision Port Form for Port Management - IP Filters Tab

Field/Button	Description
Rank	The precedence of the classifier
Classifier Name	The name of the classifier that has already been defined.
Field Match(es)	The matching rules for the classifier.
Action(s)	The actions to occur when there is a match
Port IP Filter Counters:	The counter for packets set against this classifier - Match Count - Filter Count - Policed Count
Add Classifier	Bring up the **Add Classifier to Port** Form. The data filled classifiers are listed, and the user can chose one of these and can define the precedence.
Delete Classifier	Deletes the classifier from the port
Reset Counters	Reset the counters to 0
Command History	Views the CLI commands and responses for the operations performed in the Port Management application. This is the same for all tabs.
Close	Closes the View Details application (the window as well as the tab). This is the same for all tabs.

14.14.8 Ether-Like Port (Port Log Tab)

Selecting the **Port Log** tab invokes a table that lists all the port-related management logs that have been generated. This window has the same columns as the ADSL Port Management window for Port Log.

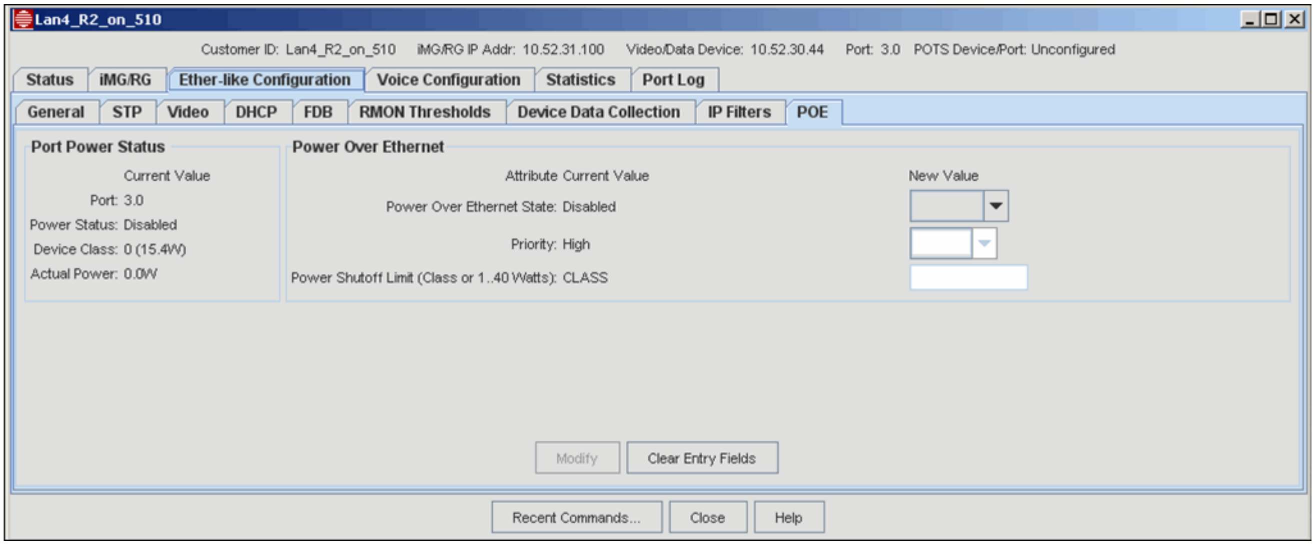
For a description of management logs and the meaning of fields, refer to the iMAP Log / Troubleshooting Manual.

14.14.9 Ether-Like Port (DS3-SFP Tab)

For iMAP 9000 series devices, a DS3 SFP is supported off of the GE3 and GE8 cards, which allows a DS3 interface and a Gigabit Ethernet interworking function. For details, refer to "DS3-SFP Support" on page 224.

14.14.10 Ether-Like Port (POE Tab)

To view and modify the settings of an Ethernet port that has POE configured, a POE tab is added, as shown in the following figure.



Customer ID: Lan4_R2_on_510 iMG/RG IP Addr: 10.52.31.100 Video/Data Device: 10.52.30.44 Port: 3.0 POTS Device/Port: Unconfigured

Port Power Status

Current Value
Port: 3.0
Power Status: Disabled
Device Class: 0 (15.4W)
Actual Power: 0.0W

Power Over Ethernet

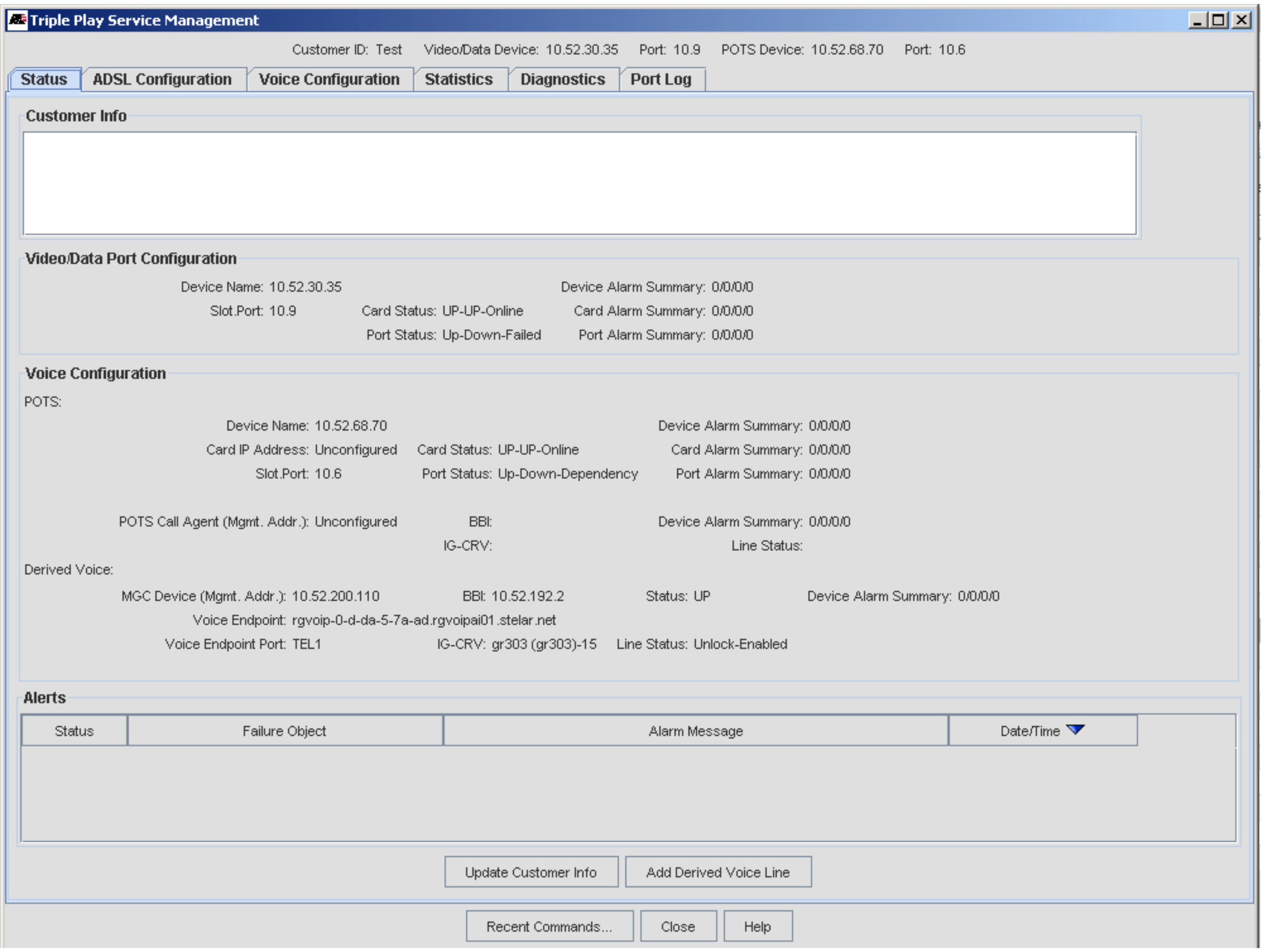
Attribute Current Value New Value
Power Over Ethernet State: Disabled
Priority: High
Power Shutoff Limit (Class or 1..40 Watts): CLASS

FIGURE 14-24 Service Management GUI for POE

14.15 ADSL Configuration Tab

14.15.1 Status Tab

The Status Tab Form is shown in Figure 14-25.



Customer ID: Test Video/Data Device: 10.52.30.35 Port: 10.9 POTS Device: 10.52.68.70 Port: 10.6

Customer Info

Video/Data Port Configuration

Device Name: 10.52.30.35 Device Alarm Summary: 0/0/0/0
Slot.Port: 10.9 Card Status: UP-UP-Online Card Alarm Summary: 0/0/0/0
Port Status: Up-Down-Failed Port Alarm Summary: 0/0/0/0

Voice Configuration

POTS:

Device Name: 10.52.68.70 Device Alarm Summary: 0/0/0/0
Card IP Address: Unconfigured Card Status: UP-UP-Online Card Alarm Summary: 0/0/0/0
Slot.Port: 10.6 Port Status: Up-Down-Dependency Port Alarm Summary: 0/0/0/0

POTS Call Agent (Mgmt. Addr.): Unconfigured BBI: Device Alarm Summary: 0/0/0/0
IG-CRV: Line Status:

Derived Voice:

MGC Device (Mgmt. Addr.): 10.52.200.110 BBI: 10.52.192.2 Status: UP Device Alarm Summary: 0/0/0/0
Voice Endpoint: rgvoip-0-d-da-5-7a-ad.rgvoipai01.stelar.net
Voice Endpoint Port: TEL1 IG-CRV: gr303 (gr303)-15 Line Status: Unlock-Enabled

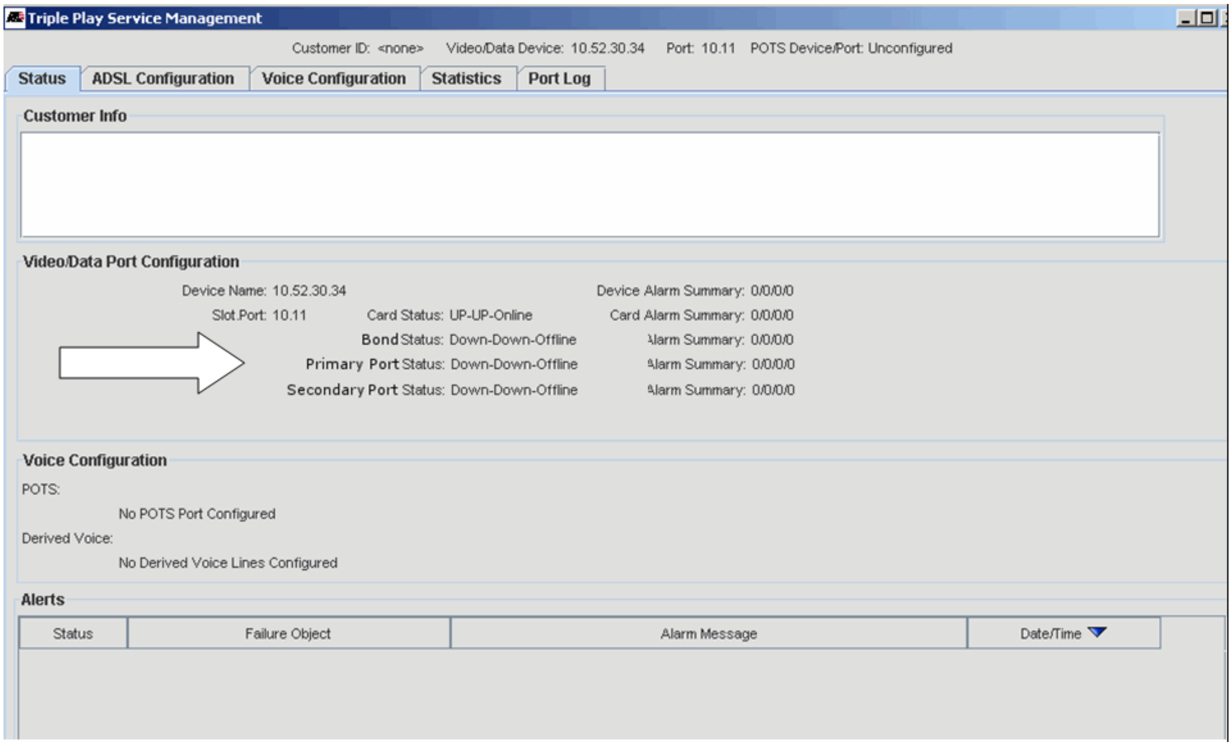
Alerts

Status	Failure Object	Alarm Message	Date/Time ▼

FIGURE 14-25 ADSL Configuration Form - Status Tab

For a data-only port using ADSL (no POTS or Derived Voice configuration), only the Video/Data Port panel has status information on the state of the port. Included is Alerts Panel that lists the current associated alarms.

If the ADSL port is part of a Bond configuration, the Port details tab is expanded to show the Bond status, as well as status of all the ADSL ports. The alerts table contains alarms for all components, device, card, bond, and ADSL ports. Refer to the following figure.



Triple Play Service Management

Customer ID: <none> Video/Data Device: 10.52.30.34 Port: 10.11 POTS Device/Port: Unconfigured

Customer Info

Video/Data Port Configuration

Device Name: 10.52.30.34 Device Alarm Summary: 0/0/0/0

Slot.Port: 10.11 Card Status: UP-UP-Online Card Alarm Summary: 0/0/0/0

Bond Status: Down-Down-Offline Alarm Summary: 0/0/0/0

Primary Port Status: Down-Down-Offline Alarm Summary: 0/0/0/0

Secondary Port Status: Down-Down-Offline Alarm Summary: 0/0/0/0

Voice Configuration

POTS:

No POTS Port Configured

Derived Voice:

No Derived Voice Lines Configured

Alerts

Status	Failure Object	Alarm Message	Date/Time

FIGURE 14-26 ADSL Status - Bonded Port

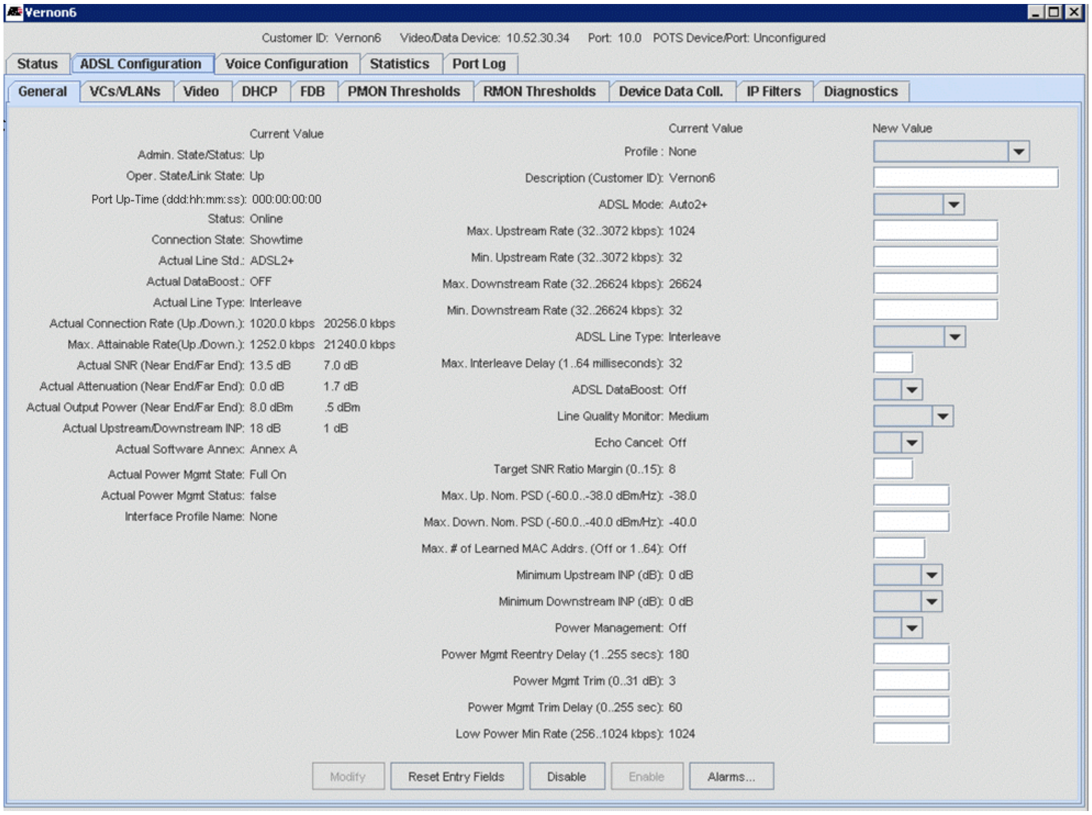
14.15.2 ADSL Configuration Tab - Overview

The ADSL Configuration tab has the following associated forms, each with its own tab:

- General
- VCs/VLANs
- Video
- DHCP
- FDB
- PMON Thresholds
- RMON Thresholds
- Device Data Coll.
- IP Filters

These are shown in the following figures. Following each figure is a table that describes the panels/fields of the form.

14.15.3 ADSL Configuration Tab - General



Customer ID: Vernon6 Video/Data Device: 10.52.30.34 Port: 10.0 POTS Device/Port: Unconfigured

	Current Value	
Admin. State/Status:	Up	
Oper. State/Link State:	Up	
Port Up-Time (ddd:hh:mm:ss):	000:00:00:00	
Status:	Online	
Connection State:	Showtime	
Actual Line Std.:	ADSL2+	
Actual DataBoost.:	OFF	
Actual Line Type:	Interleave	
Actual Connection Rate (Up./Down.):	1020.0 kbps	20256.0 kbps
Max. Attainable Rate(Up./Down.):	1252.0 kbps	21240.0 kbps
Actual SNR (Near End/Far End):	13.5 dB	7.0 dB
Actual Attenuation (Near End/Far End):	0.0 dB	1.7 dB
Actual Output Power (Near End/Far End):	8.0 dBm	.5 dBm
Actual Upstream/Downstream INP:	18 dB	1 dB
Actual Software Annex:	Annex A	
Actual Power Mgmt State:	Full On	
Actual Power Mgmt Status:	false	
Interface Profile Name:	None	

	Current Value	New Value
Profile :	None	
Description (Customer ID):	Vernon6	
ADSL Mode:	Auto2+	
Max. Upstream Rate (32..3072 kbps):	1024	
Min. Upstream Rate (32..3072 kbps):	32	
Max. Downstream Rate (32..26624 kbps):	26624	
Min. Downstream Rate (32..26624 kbps):	32	
ADSL Line Type:	Interleave	
Max. Interleave Delay (1..64 milliseconds):	32	
ADSL DataBoost:	Off	
Line Quality Monitor:	Medium	
Echo Cancel:	Off	
Target SNR Ratio Margin (0..15):	8	
Max. Up. Nom. PSD (-60.0..-38.0 dBm/Hz):	-38.0	
Max. Down. Nom. PSD (-60.0..-40.0 dBm/Hz):	-40.0	
Max. # of Learned MAC Addrs. (Off or 1..64):	Off	
Minimum Upstream INP (dB):	0 dB	
Minimum Downstream INP (dB):	0 dB	
Power Management:	Off	
Power Mgmt Reentry Delay (1..255 secs):	180	
Power Mgmt Trim (0..31 dB):	3	
Power Mgmt Trim Delay (0..255 sec):	60	
Low Power Min Rate (256..1024 kbps):	1024	

FIGURE 14-27 ADSL Configuration Form - General Tab

TABLE 14-11 ADSL Configuration Form, General Tab

Field/Button	Description
Admin. State	The Administrative State can be controlled and determines the Operational State.
Oper. State/Link State	The ability of the port to provide service. The Administrative State must be up and then the system determines if the port can provide service.
Port Up-Time	Amount of time the physical interface has been in the UP-UP-Online state.
Status	The status of the port that follows form the Administrative State and Operational State. For meanings, refer to the *Software Reference for iMAP Series Switches*. - ONLINE - IN TEST - FAILED - OFFLINE - DEPENDENCY - DEGRADED - NOT INSTALLED - INITIALIZATION REQUIRED - TERMINATING
Connection State	The connection state, such as Idle or Showtime

TABLE 14-11 ADSL Configuration Form, General Tab (Continued)

Field/Button	Description
Actual Line Std.	The line standard that was actually chosen.
Actual Databoost	Whether the DATABOOST feature has been implemented
Actual Line Type	The line type that was actually chosen.
Actual Upstream/ Downstream Rate	The upstream/downstream rate that was actually attained.
Max. Attainable Upstream/ Downstream Rate	The possible upstream/downstream rate according to dsl type and mode.
Actual SNR (Near End/Far End)	The signal-noise ratio for near end/far end that was actually attained.
Actual Attenuation (Near End/Far End)	The attenutation for near end/far end that was actually attained.
Actual Output Power (Near End/Far End)	The output power achieved for near end/far end.
Actual Software Annex	The Annex (A, B, or C) that is being used
Actual Power Mgmt State	The state the interface is in for power reduction (Full On, Low Power, Idle)
Actual Power Mgmt Status	Whether the power management feature has been activated for the interface
Actual Upstream INP	The actual impulse noise protection value for upstream
Actual Downstream INP	The actual impulse noise protection value for downstream
Profile	Which profile is being used (AutoProv or none, which uses default values).
Description (Customer ID)	An ID that can be given to uniquely identify the port. In most cases, the subscriber's telephone number is used. Refer to "Naming Convention for Customer IDs (Triple Play Form)" on page 780.
Max. Upstream Rate	The maximum upstream rate that is provisioned.
Min. Upstream Rate	The minimum upstream rate that is provisioned.
Max. Downstream Rate	The maximum downstream rate that is provisioned.
Min. Downstream Rate	The minimum downstream rate that is provisioned.
Target SNR Margin	Specifies the target signal-to-noise ratio (in dB) to achieve on an ADSL port.
ADSL Line Type	Specifies the ADSL line type as per ITU G.992. Allowed values are FAST and INTERLEAVE, although FAST is not allowed if the MODE is GLITE. Refer to the iMAP User's Guide, Section 4.
ADSL Mode	Specifies the ADSL line mode standard. Refer to the *Software Reference for iMAP Series Switches*.
ADSL Databoost	Whether the Databoost feature has been provisioned
Line Quality Monitor	The level the line quality monitor has been set at. Refer to the *Software Reference for iMAP Series Switches*.
Max. Interleave Delay	Specifies the maximum interleave delay in milliseconds used when the ADSL linetype is set to INTERLEAVE. Refer to the *Software Reference for iMAP Series Switches*.
Echo Cancel	Specifies whether echo cancellation is utilized on ADSL ports running G.DMT mode as per ITU-T. Refer to the *Software Reference for iMAP Series Switches*.
Max. # of Learned MAC Addresses	Depending on feature provisioning, the number of MAC addresses that can be learned (or Off)
Minimum Upstream INP	Sets the minimum impulse noise protection value for upstream.
Minimum Downstream INP	Sets the minimum impulse noise protection value for downstream.

TABLE 14-11 ADSL Configuration Form, General Tab (Continued)

Field/Button	Description
Power Management	Changes the current power management state.
Power Mgmt Reentry Delay	The amount of time that must elapse before re-entering the Low Power state after a transition to the Full On state. (Should not be set to a value less than 120 seconds)
Power Mgmt Trim	The maximum aggregate transmit power reduction (trimming) that can be performed with each power trim operation in the Low Power state.
Power Mgmt Trim Delay	The amount of time that must elapse before an additional reduction (trimming) of power occurs in the Low Power state.
Low Power Min Rate	The minimum net data rate for the bearer channel while operating in the Low Power state. The value for LOWPOWERRATE must be between MAXDOWNSTREAMRATE and MINDOWNSTREAMRATE
Max. Upstream Nominal PSD	VDSL/ADSL power spectrum density limits are defined by the band plan and determine this value.
Max. Downstream Nominal PSD	VDSL/ADSL power spectrum density limits are defined by the band plan and determine this value.
Modify	Enabled when a value in New Value field has been entered, modifies the attributes according to the updated values.There is an error message if a value is invalid.
Clear Entry Fields	Clear any fields that have been datafilled but not yet Modified
Enable	Enabled if the port is in an Administrative State of DOWN, enables the port and so brings the Administrative State to UP. If possible (for example, the ADSL card must be enabled), the Operational State will change to UP.
Disable	Enabled if the port is in an Administrative State of UP, disables the port and so brings the Administrative State to DOWN. The Operational State will also change to DOWN.
Alarms	Invokes the Alarm table of the Fault Management Object.

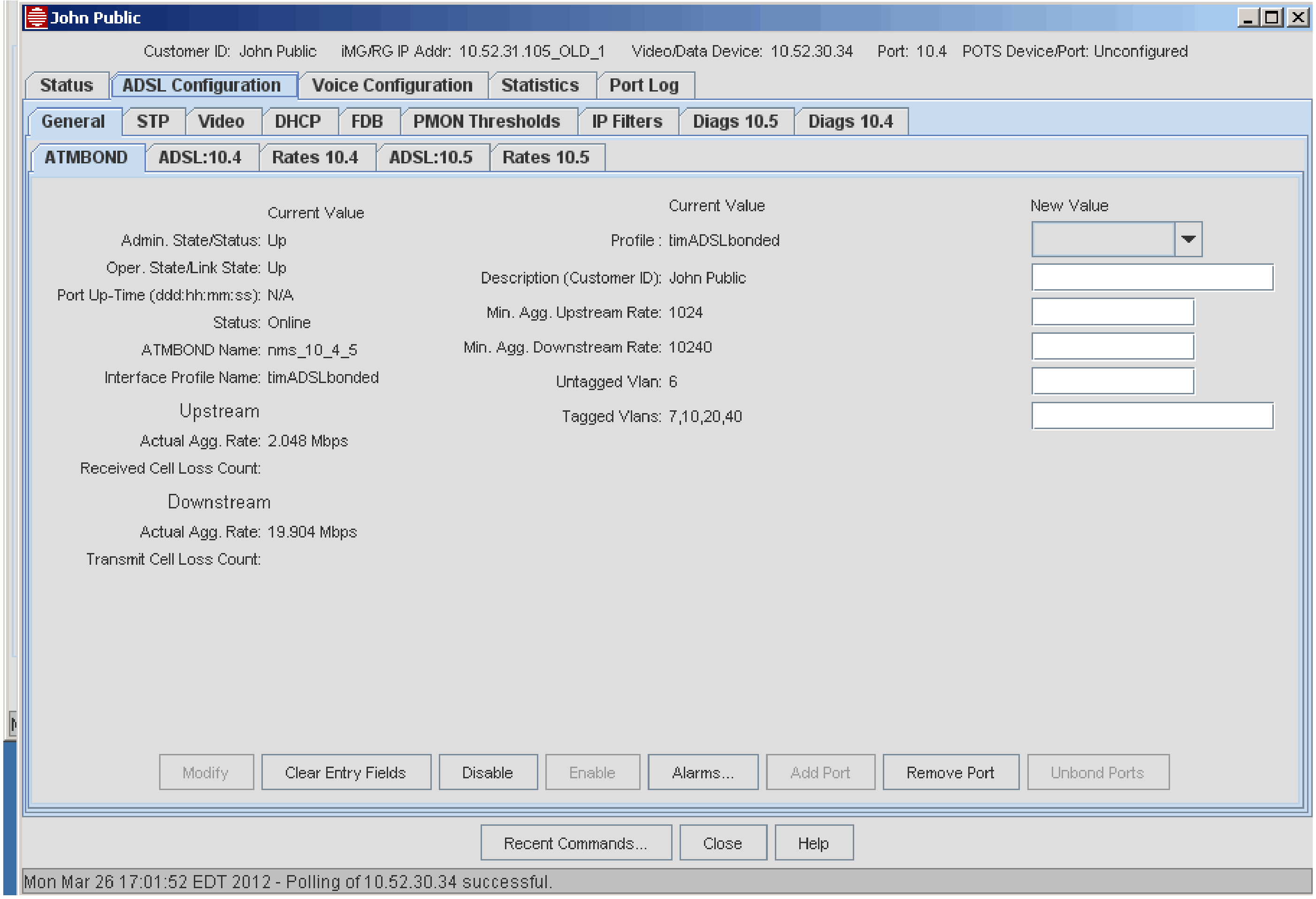
The values on this form can be modified as follows:

Note: This requires that the port be disabled, which will interrupt service on the port.

1. Click **Disable** to disable the port. A dialog box will appear warning you that service on the port will be interrupted. If you wish to proceed, click **Yes**.
2. Modify the information as needed.
3. Click **Modify** to save the changes.
4. Click **Enable** to re-enable the port.

For an ADSL Bonded port, the General Tab of the Port Details window contains information about the ATMBond. Each ADSL port that belong to the bond group has its own tab. There is the button on the panel “Add Bonded Port.”, to allow adding another port to the group. This button is disabled when the group is full. Refer to the following figures.

Note: Currently only two pairs can be bonded, but a group can be created with only one pair.



Customer ID: John Public iMG/RG IP Addr: 10.52.31.105_OLD_1 Video/Data Device: 10.52.30.34 Port: 10.4 POTS Device/Port: Unconfigured

Admin. State/Status: Up
Oper. State/Link State: Up
Port Up-Time (ddd:hh:mm:ss): N/A
Status: Online
ATMBOND Name: nms_10_4_5
Interface Profile Name: timADSLbonded

Upstream
Actual Agg. Rate: 2.048 Mbps
Received Cell Loss Count:

Downstream
Actual Agg. Rate: 19.904 Mbps
Transmit Cell Loss Count:

Profile : timADSLbonded
Description (Customer ID): John Public
Min. Agg. Upstream Rate: 1024
Min. Agg. Downstream Rate: 10240
Untagged Vlan: 6
Tagged Vlans: 7,10,20,40

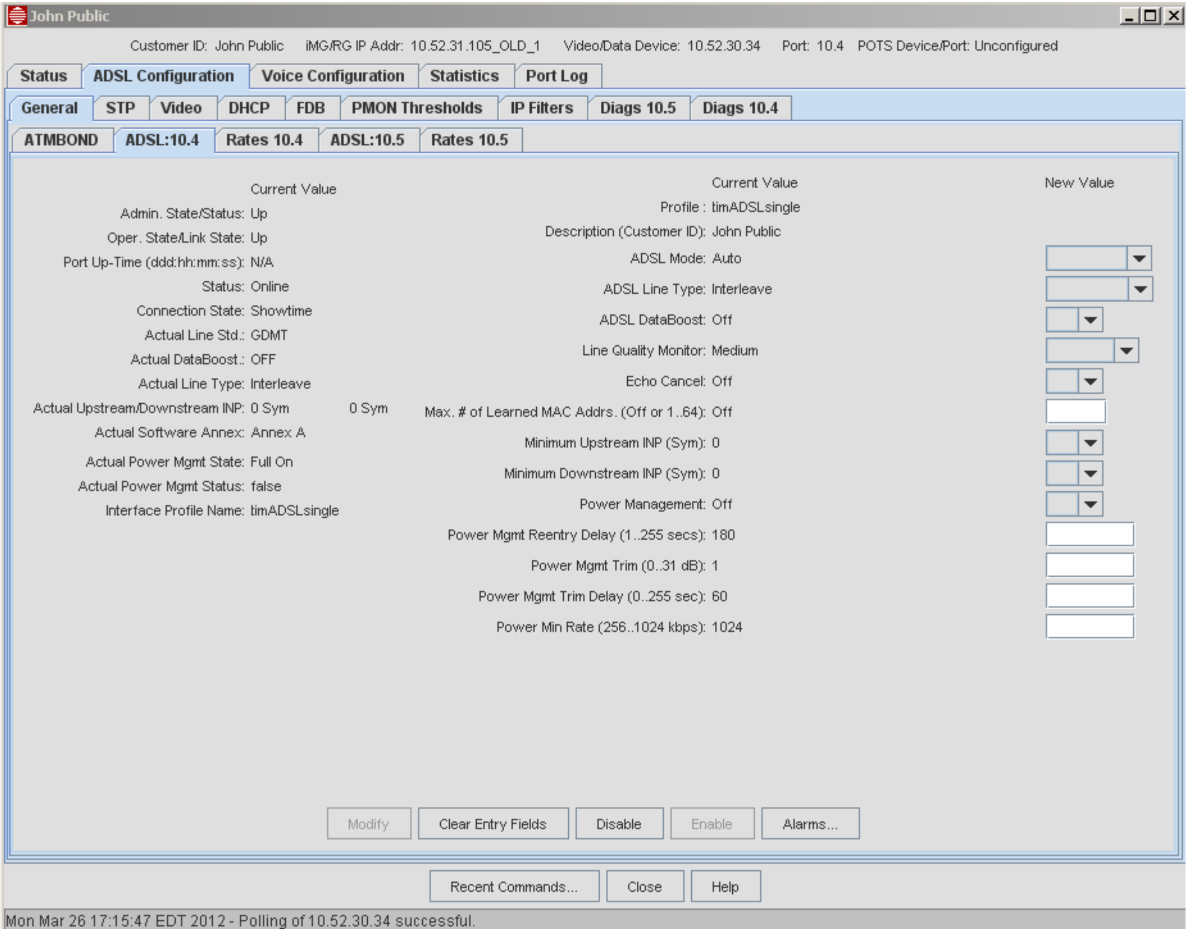
Mon Mar 26 17:01:52 EDT 2012 - Polling of 10.52.30.34 successful.

FIGURE 14-28 ADSL General Tab with ATM Bond Attributes

Each ADSL port has it's own general tab and rates tab. The values for the Profile name and Customer ID are from the Triple_play provisioning form (refer to TBS). Some fields that appear on a regular ADSL port's general tab are moved to the ATMBOND tab since they are tied to the Bond rather than the port.

For more information on the configuration options for the Bonding and the Disable (Bond) and Remove Port options, refer to Figure 14.29.

Refer to the following



Customer ID: John Public iMG/RG IP Addr: 10.52.31.105_OLD_1 Video/Data Device: 10.52.30.34 Port: 10.4 POTS Device/Port: Unconfigured

Current Value

Admin. State/Status: Up
Oper. State/Link State: Up
Port Up-Time (ddd:hh:mm:ss): N/A
Status: Online
Connection State: Showtime
Actual Line Std.: GDMT
Actual DataBoost.: OFF
Actual Line Type: Interleave
Actual Upstream/Downstream INP: 0 Sym 0 Sym
Actual Software Annex: Annex A
Actual Power Mgmt State: Full On
Actual Power Mgmt Status: false
Interface Profile Name: timADSLsingle

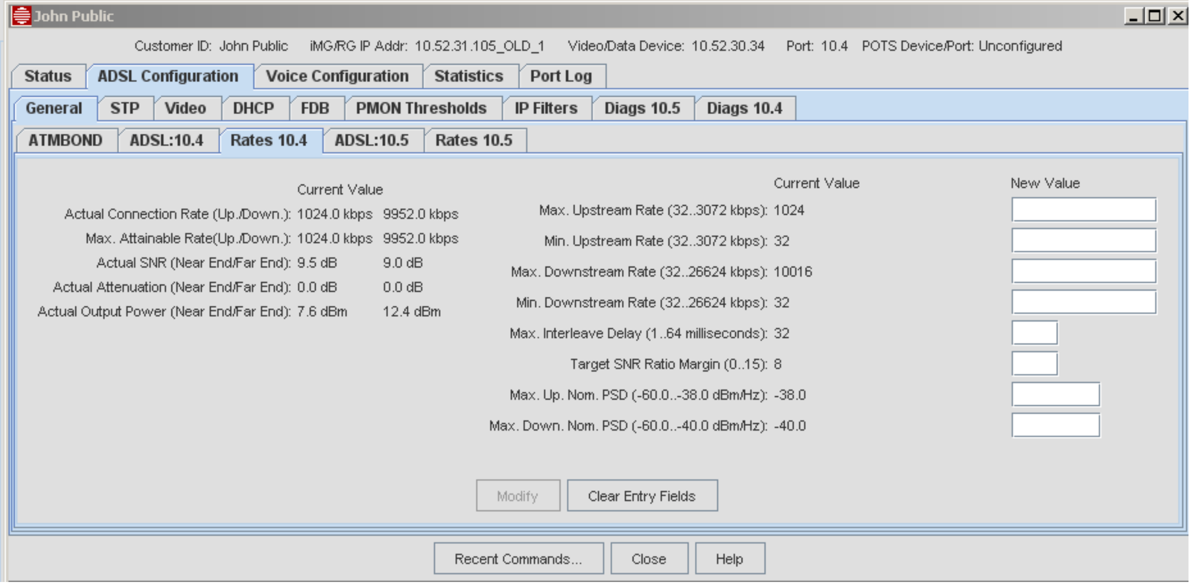
Current Value New Value

Profile : timADSLsingle
Description (Customer ID): John Public
ADSL Mode: Auto
ADSL Line Type: Interleave
ADSL DataBoost: Off
Line Quality Monitor: Medium
Echo Cancel: Off
Max. # of Learned MAC Addrs. (Off or 1..64): Off
Minimum Upstream INP (Sym): 0
Minimum Downstream INP (Sym): 0
Power Management: Off
Power Mgmt Reentry Delay (1..255 secs): 180
Power Mgmt Trim (0..31 dB): 1
Power Mgmt Trim Delay (0..255 sec): 60
Power Min Rate (256..1024 kbps): 1024

Mon Mar 26 17:15:47 EDT 2012 - Polling of 10.52.30.34 successful.

figu

FIGURE 14-29 ADSL General Tab with ATM Bond - Single Port Attributes



Customer ID: John Public iMG/RG IP Addr: 10.52.31.105_OLD_1 Video/Data Device: 10.52.30.34 Port: 10.4 POTS Device/Port: Unconfigured

Current Value

Actual Connection Rate (Up./Down.): 1024.0 kbps 9952.0 kbps
Max. Attainable Rate(Up./Down.): 1024.0 kbps 9952.0 kbps
Actual SNR (Near End/Far End): 9.5 dB 9.0 dB
Actual Attenuation (Near End/Far End): 0.0 dB 0.0 dB
Actual Output Power (Near End/Far End): 7.6 dBm 12.4 dBm

Current Value New Value

Max. Upstream Rate (32..3072 kbps): 1024
Min. Upstream Rate (32..3072 kbps): 32
Max. Downstream Rate (32..26624 kbps): 10016
Min. Downstream Rate (32..26624 kbps): 32
Max. Interleave Delay (1..64 milliseconds): 32
Target SNR Ratio Margin (0..15): 8
Max. Up. Nom. PSD (-60.0..-38.0 dBm/Hz): -38.0
Max. Down. Nom. PSD (-60.0..-40.0 dBm/Hz): -40.0

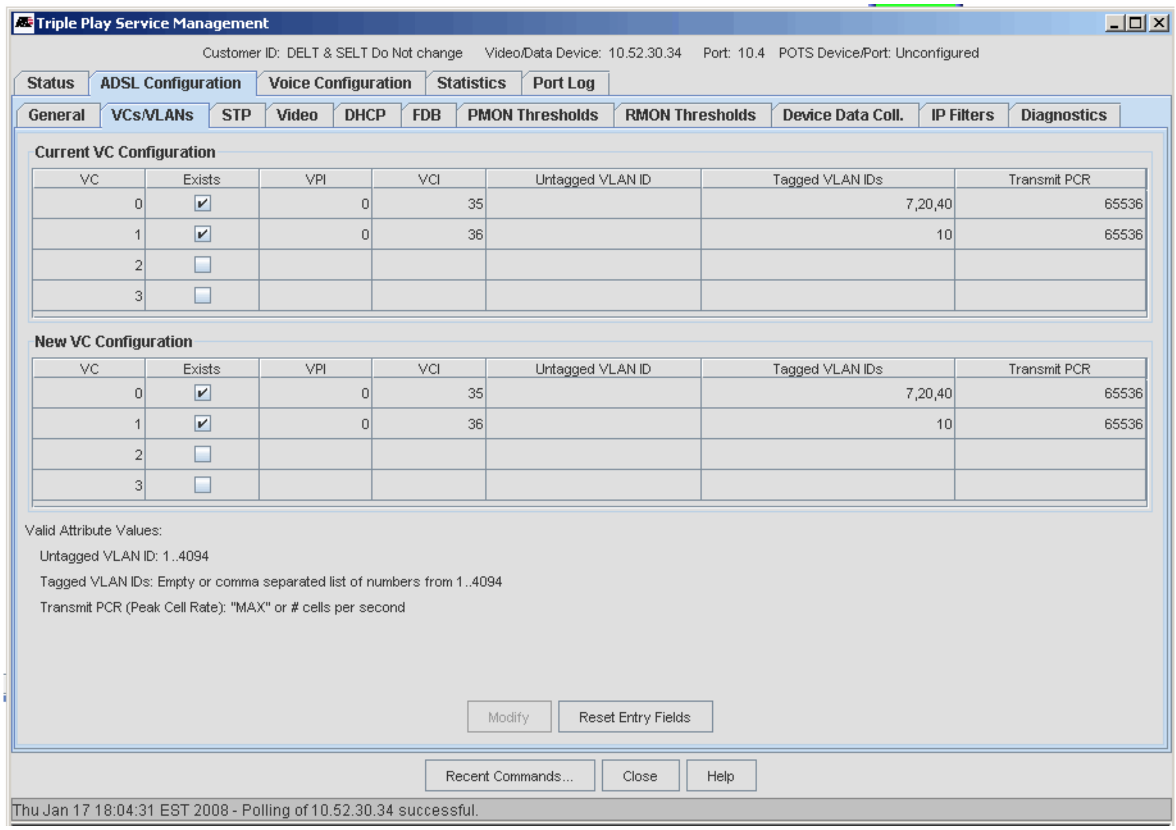
FIGURE 14-30 ADSL General Tab with ATM Bond - Single Port Rate Attributes

14.15.4 ADSL Configuration Tab - VCs/VLANs

The ability to correlate the port to Virtual Channels (VCs) and then the VC to one or more VLANs is configured through this tab.

Note: The ADSL16 and ADSL8S cards allow up to four VCs to be configured per port, while the ADSL24 card allows only one VC per port. The ADSL24A/B card supports 4 VCs.

Figure 14-36 shows the ADSL statistics once they have been enabled.



Customer ID: DELT & SELT Do Not change Video/Data Device: 10.52.30.34 Port: 10.4 POTS Device/Port: Unconfigured

Current VC Configuration

VC	Exists	VPI	VCI	Untagged VLAN ID	Tagged VLAN IDs	Transmit PCR
0	☑	0	35		7,20,40	65536
1	☑	0	36		10	65536
2	☐					
3	☐					

New VC Configuration

VC	Exists	VPI	VCI	Untagged VLAN ID	Tagged VLAN IDs	Transmit PCR
0	☑	0	35		7,20,40	65536
1	☑	0	36		10	65536
2	☐					
3	☐					

Valid Attribute Values:

Untagged VLAN ID: 1..4094

Tagged VLAN IDs: Empty or comma separated list of numbers from 1..4094

Transmit PCR (Peak Cell Rate): "MAX" or # cells per second

Thu Jan 17 18:04:31 EST 2008 - Polling of 10.52.30.34 successful.

FIGURE 14-31 ADSL Configuration Form - VC/VLANs Tab

TABLE 14-12 View Details Form, VCs/VLANs Tab

Field/Button	Description
Current VC Configuration	The current values for all attributes of the VC configuration. These fields are view-only.
New VC Configuration	Initially this has a copy of the current configuration, but the fields are editable. The best strategy to fill in a new VC is to click on the Exists tic box and the appropriate values for the other columns are filled in.
Valid Attribute Values	Guidelines for valid attributes values or ranges.
Modify	Makes the changes made in the New VC Configuration Fields. Error messages appear if there are any invalid values.
Reset Changes	Reverts to the current VC configuration.

14.15.5 ADSL Video Tab

Refer to "Video Tab" on page 485.

14.15.6 ADSL Configuration Tab - DHCP Tab

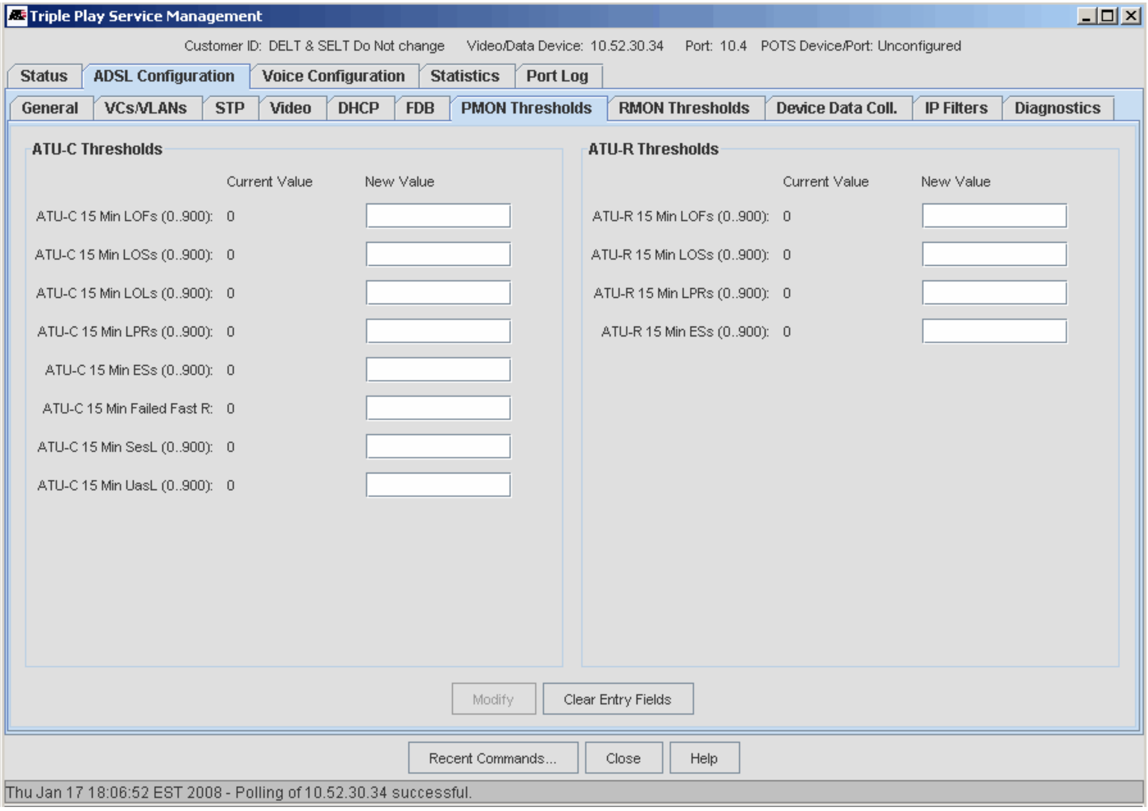
Refer to "DHCP Tab" on page 485.

14.15.7 ADSL Configuration Tab - FDB Tab

Refer to "FDB Tab" on page 485.

14.15.8 ADSL Configuration Tab - PMON Thresholds Tab

Selecting the **PMON Thresholds** tab brings up a form (Figure 14-32) that allows thresholds to be set for the ATU-C and ATU-R statistics. When a threshold is crossed, an ADSL Port Log occurs, which will appear in the ADSL Port Log tab, and that is the only time the alert is produced during the 15 minute or 24 -hour period. Also, the device sends a trap, which is processed by Alarm Management so that an alarm is displayed.



Customer ID: DELT & SELT Do Not change Video/Data Device: 10.52.30.34 Port: 10.4 POTS Device/Port: Unconfigured

ATU-C Thresholds

	Current Value	New Value
ATU-C 15 Min LOFs (0..900):	0	
ATU-C 15 Min LOSs (0..900):	0	
ATU-C 15 Min LOLs (0..900):	0	
ATU-C 15 Min LPRs (0..900):	0	
ATU-C 15 Min ESs (0..900):	0	
ATU-C 15 Min Failed Fast R:	0	
ATU-C 15 Min SesL (0..900):	0	
ATU-C 15 Min UasL (0..900):	0	

ATU-R Thresholds

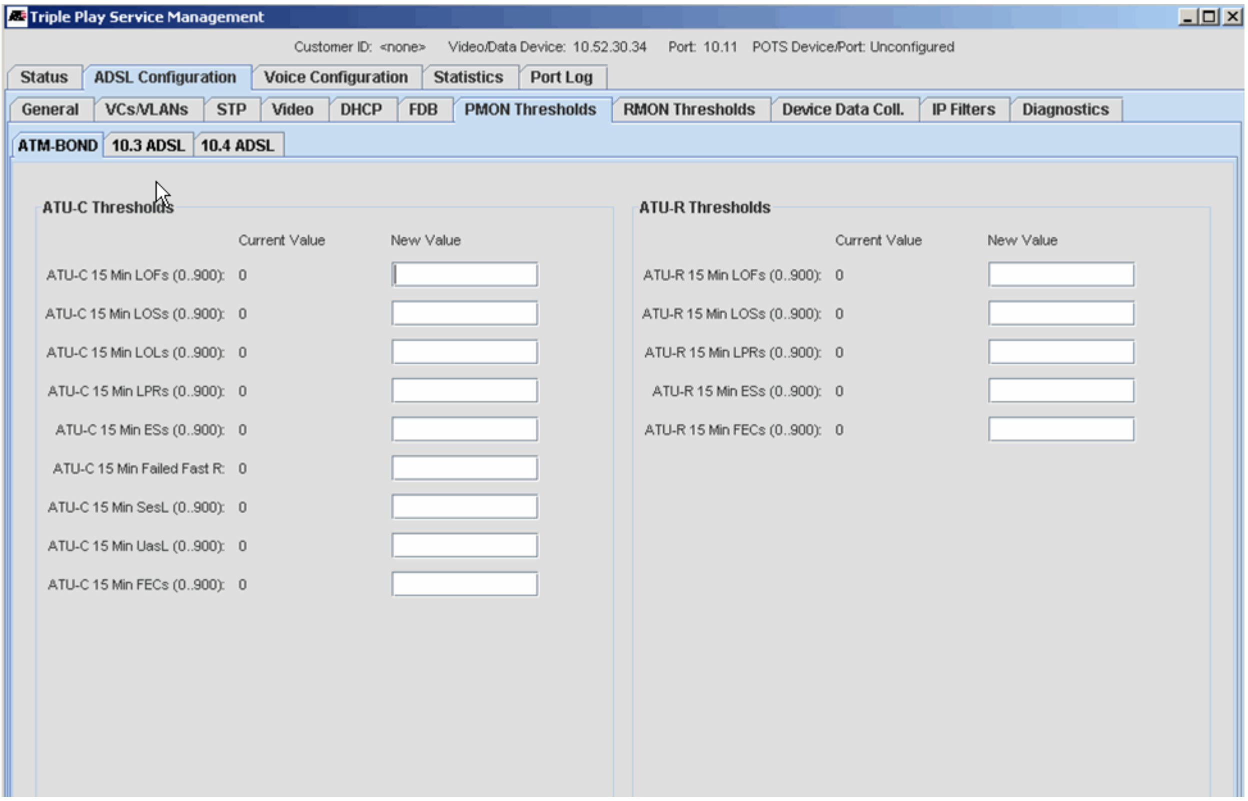
	Current Value	New Value
ATU-R 15 Min LOFs (0..900):	0	
ATU-R 15 Min LOSs (0..900):	0	
ATU-R 15 Min LPRs (0..900):	0	
ATU-R 15 Min ESs (0..900):	0	

Thu Jan 17 18:06:52 EST 2008 - Polling of 10.52.30.34 successful.

FIGURE 14-32 ADSL Configuration Form - PMON Thresholds Tab

The threshold values can be modified by typing in new values in each field as needed and then clicking **Modify**.

For ADSL Bonding, PMON statistics can be collected for each Interface. RMONs are tied to the Bond interface. Refer to the following figure.



Customer ID: <none> Video/Data Device: 10.52.30.34 Port: 10.11 POTS Device/Port: Unconfigured

ATU-C Thresholds

	Current Value	New Value
ATU-C 15 Min LOFs (0..900):	0	
ATU-C 15 Min LOSs (0..900):	0	
ATU-C 15 Min LOLs (0..900):	0	
ATU-C 15 Min LPRs (0..900):	0	
ATU-C 15 Min ESs (0..900):	0	
ATU-C 15 Min Failed Fast R:	0	
ATU-C 15 Min SesL (0..900):	0	
ATU-C 15 Min UasL (0..900):	0	
ATU-C 15 Min FECs (0..900):	0	

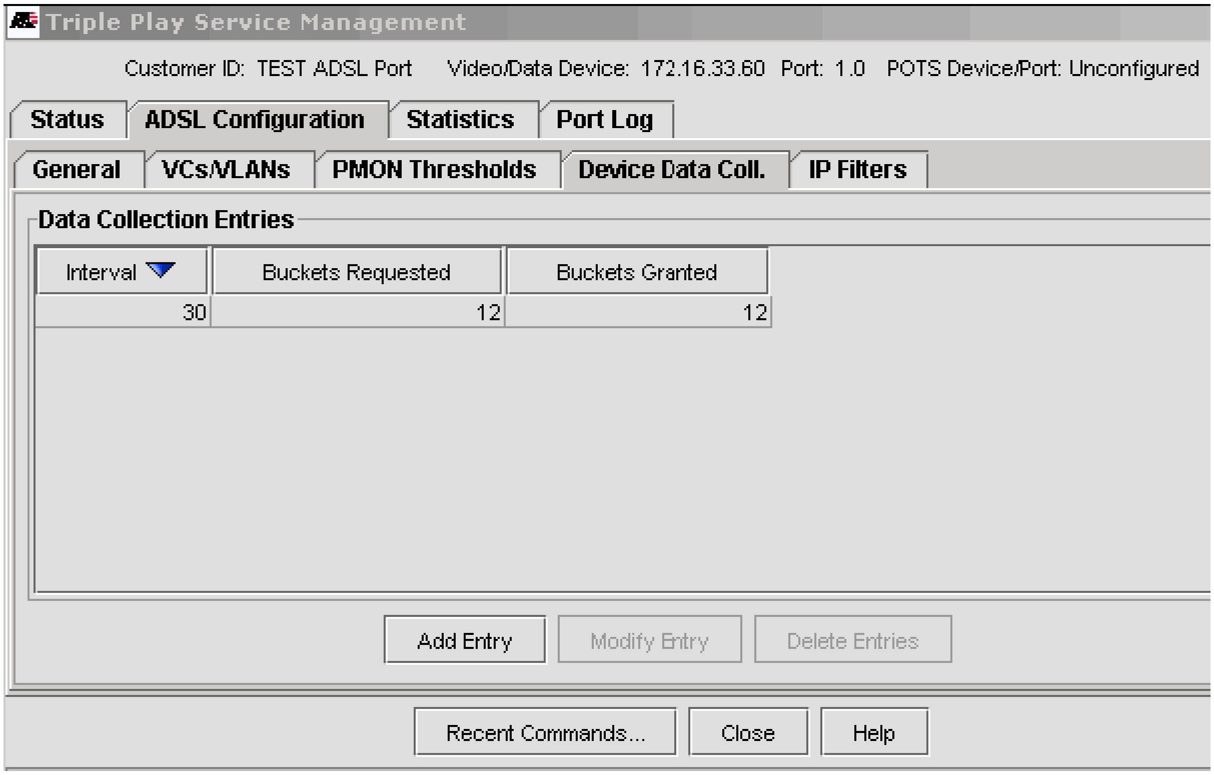
ATU-R Thresholds

	Current Value	New Value
ATU-R 15 Min LOFs (0..900):	0	
ATU-R 15 Min LOSs (0..900):	0	
ATU-R 15 Min LPRs (0..900):	0	
ATU-R 15 Min ESs (0..900):	0	
ATU-R 15 Min FECs (0..900):	0	

FIGURE 14-33 ADSL Bonding - PMON Thresholds

14.15.9 ADSL Configuration Tab - Device Data Collection Tab

The Device Data Collection form is a way to configure buckets that will collect statistics and the interval at which they are filled.



Customer ID: TEST ADSL Port Video/Data Device: 172.16.33.60 Port: 1.0 POTS Device/Port: Unconfigured

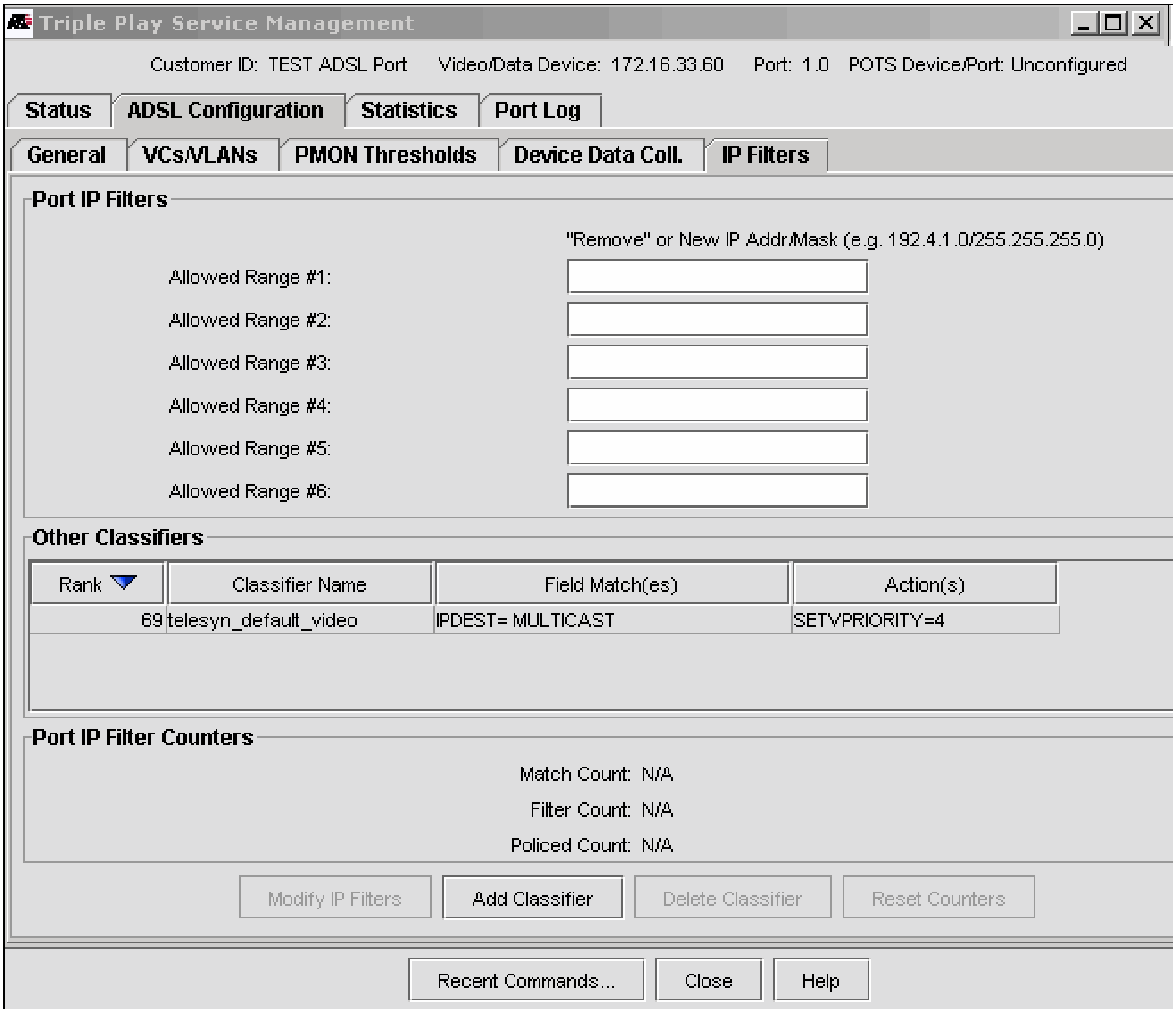
Interval	Buckets Requested	Buckets Granted
30	12	12

FIGURE 14-34 ADSL Configuration Form - Device Data Coll. Tab

The Add History brings up a form that allows the user to enter the number of buckets to be configured and at what interval (in seconds).

14.15.10 ADSL Configuration Tab - IP Filters

Incoming data to the ADSL ports (the ingress ports) can be filtered by IP address or a range of IP addresses. Figure 14-35 shows the IP Filters tab, while Table 14-13 shows the buttons and fields available. Refer to the *Software Reference for iMAP Series Switches* for details.



Customer ID: TEST ADSL Port Video/Data Device: 172.16.33.60 Port: 1.0 POTS Device/Port: Unconfigured

Port IP Filters

"Remove" or New IP Addr/Mask (e.g. 192.4.1.0/255.255.255.0)

Allowed Range #1:

Allowed Range #2:

Allowed Range #3:

Allowed Range #4:

Allowed Range #5:

Allowed Range #6:

Other Classifiers

Rank ▼	Classifier Name	Field Match(es)	Action(s)
69	telesyn_default_video	IPDEST= MULTICAST	SETVPRIORITY=4

Port IP Filter Counters

Match Count: N/A

Filter Count: N/A

Policed Count: N/A

FIGURE 14-35 ADSL Configuration Form - IP Filters Tab

TABLE 14-13 IP Filters Form

Field/Button	Description
Port IP Filters	Rank - Also called precedence, it is the rank a precedence a classifier has in a port. The highest rank is 1, and then in descending order. IP Filtering should have a precedence of 51-69. Classifier Name - This is the name given to the grouping of IP addresses or range of addresses. Field Match(es) - The range of IPSOURCE addresses is specified as a subnet and a mask. Action(s) -Perform actions when the incoming packet address matches what is set in the classifier: - DROP - Discard the packet. - FORWARD - Allow the packet to be forwarded. - COUNT starts the counting of the actions (DROP or FORWARD) for the classifier(s).
Port IP Counters	Match Count Filter Count Policed Count
Add Classifier	Associates a classifier with a port and give it a precedence. *Note: A port cannot have more than one rank number, even if the rank numbers belong to different classifiers.*
Delete Classifier	Delete the classifier for the port.
Reset Counters	Reset all the counters on the port to 0.

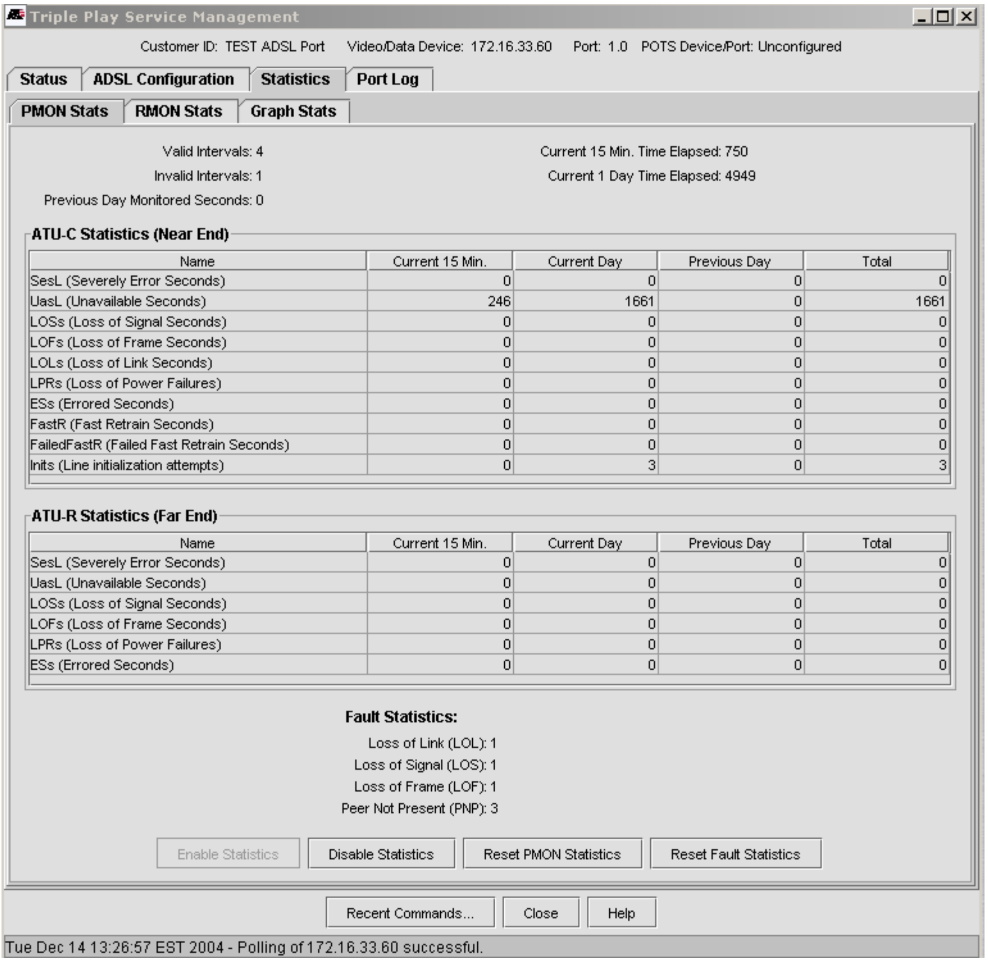
14.15.11 ADSL Statistics Tab - Overview

Performance Management is the collection of traffic statistics over the interfaces (usually ports) over a specified time period (called the interval). Thresholds can be set so that if the value for a certain statistic crosses a threshold value, a log or alarm is produced.

14.15.12 ADSL Statistics Tab - PMON Stats Tab

Figure 14-36 shows the PMON Stats form.

Note: By default, ports are disabled for statistics and must be explicitly enabled. (Selecting the Enable Statistics button on the ADSL Statistics tab form will invoke a table of all statistics, while selecting the Disable Statistics button will delete the table.



Customer ID: TEST ADSL Port Video/Data Device: 172.16.33.60 Port: 1.0 POTS Device/Port: Unconfigured

Valid Intervals: 4
Invalid Intervals: 1
Previous Day Monitored Seconds: 0

Current 15 Min. Time Elapsed: 750
Current 1 Day Time Elapsed: 4949

ATU-C Statistics (Near End)

Name	Current 15 Min.	Current Day	Previous Day	Total
SesL (Severely Error Seconds)	0	0	0	0
UasL (Unavailable Seconds)	246	1661	0	1661
LOSs (Loss of Signal Seconds)	0	0	0	0
LOFs (Loss of Frame Seconds)	0	0	0	0
LOLs (Loss of Link Seconds)	0	0	0	0
LPRs (Loss of Power Failures)	0	0	0	0
ESs (Errored Seconds)	0	0	0	0
FastR (Fast Retrain Seconds)	0	0	0	0
FailedFastR (Failed Fast Retrain Seconds)	0	0	0	0
Inits (Line initialization attempts)	0	3	0	3

ATU-R Statistics (Far End)

Name	Current 15 Min.	Current Day	Previous Day	Total
SesL (Severely Error Seconds)	0	0	0	0
UasL (Unavailable Seconds)	0	0	0	0
LOSs (Loss of Signal Seconds)	0	0	0	0
LOFs (Loss of Frame Seconds)	0	0	0	0
LPRs (Loss of Power Failures)	0	0	0	0
ESs (Errored Seconds)	0	0	0	0

Fault Statistics:

Loss of Link (LOL): 1
Loss of Signal (LOS): 1
Loss of Frame (LOF): 1
Peer Not Present (PNP): 3

Tue Dec 14 13:26:57 EST 2004 - Polling of 172.16.33.60 successful.

FIGURE 14-36 ADSL Statistics Form - PMON Stats Tab

The ATU-C and ATU-R statistics have the following measurements:

- Valid Intervals
- Invalid Intervals
- Previous Day Monitored Seconds
- Current 15 min. Time Elapsed
- Current 1 Day Time Elapsed

The table for each statistic type gives the count for the periods.

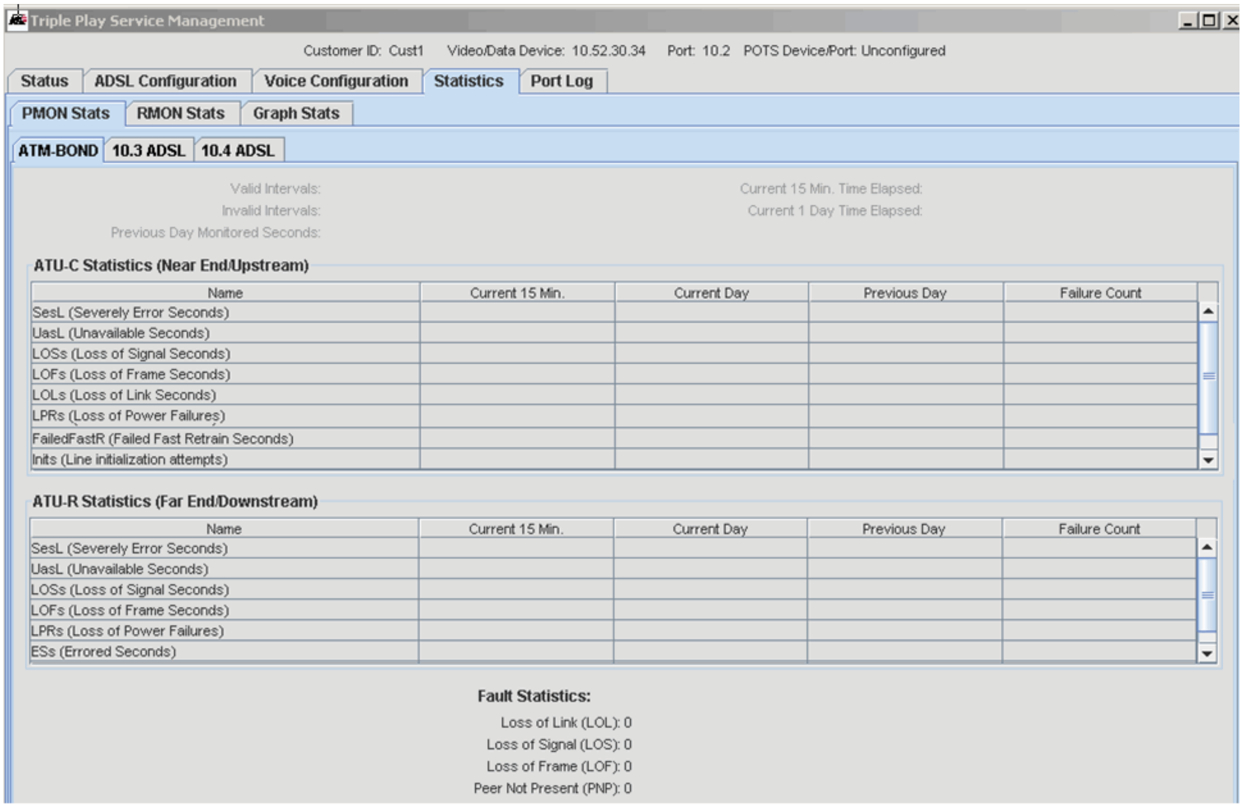
The Fault Statistics are counters, which are part of the ATN Enterprise MIB, that help to monitor the ADSL port by incrementing continuously until reset. By doing this, the history of certain events can be shown over time in order to obtain a more accurate view of what is happening with the ADSL port.

No management logs are produced with these counters, since they are cumulative, and so logs are produced for each individual event.

These counters can be reset to 0 by selecting **Reset Fault Statistics**.

Refer to the *Software Reference for iMAP Series Switches* for details about these counters.

For ADSL Bonding, PMON statistics can be collected for each Interface. Refer to the following figure.



Customer ID: Cust1 Video/Data Device: 10.52.30.34 Port: 10.2 POTS Device/Port: Unconfigured

Valid Intervals:
Invalid Intervals:
Previous Day Monitored Seconds:

Current 15 Min. Time Elapsed:
Current 1 Day Time Elapsed:

ATU-C Statistics (Near End/Upstream)

Name	Current 15 Min.	Current Day	Previous Day	Failure Count
SesL (Severely Error Seconds)				
UasL (Unavailable Seconds)				
LOSs (Loss of Signal Seconds)				
LOFs (Loss of Frame Seconds)				
LOLs (Loss of Link Seconds)				
LPRs (Loss of Power Failures)				
FailedFastR (Failed Fast Retrain Seconds)				
Inits (Line initialization attempts)				

ATU-R Statistics (Far End/Downstream)

Name	Current 15 Min.	Current Day	Previous Day	Failure Count
SesL (Severely Error Seconds)				
UasL (Unavailable Seconds)				
LOSs (Loss of Signal Seconds)				
LOFs (Loss of Frame Seconds)				
LPRs (Loss of Power Failures)				
ESs (Errored Seconds)				

Fault Statistics:

Loss of Link (LOL): 0
Loss of Signal (LOS): 0
Loss of Frame (LOF): 0
Peer Not Present (PNP): 0

FIGURE 14-37 PMON Stats - ADSL Bonding

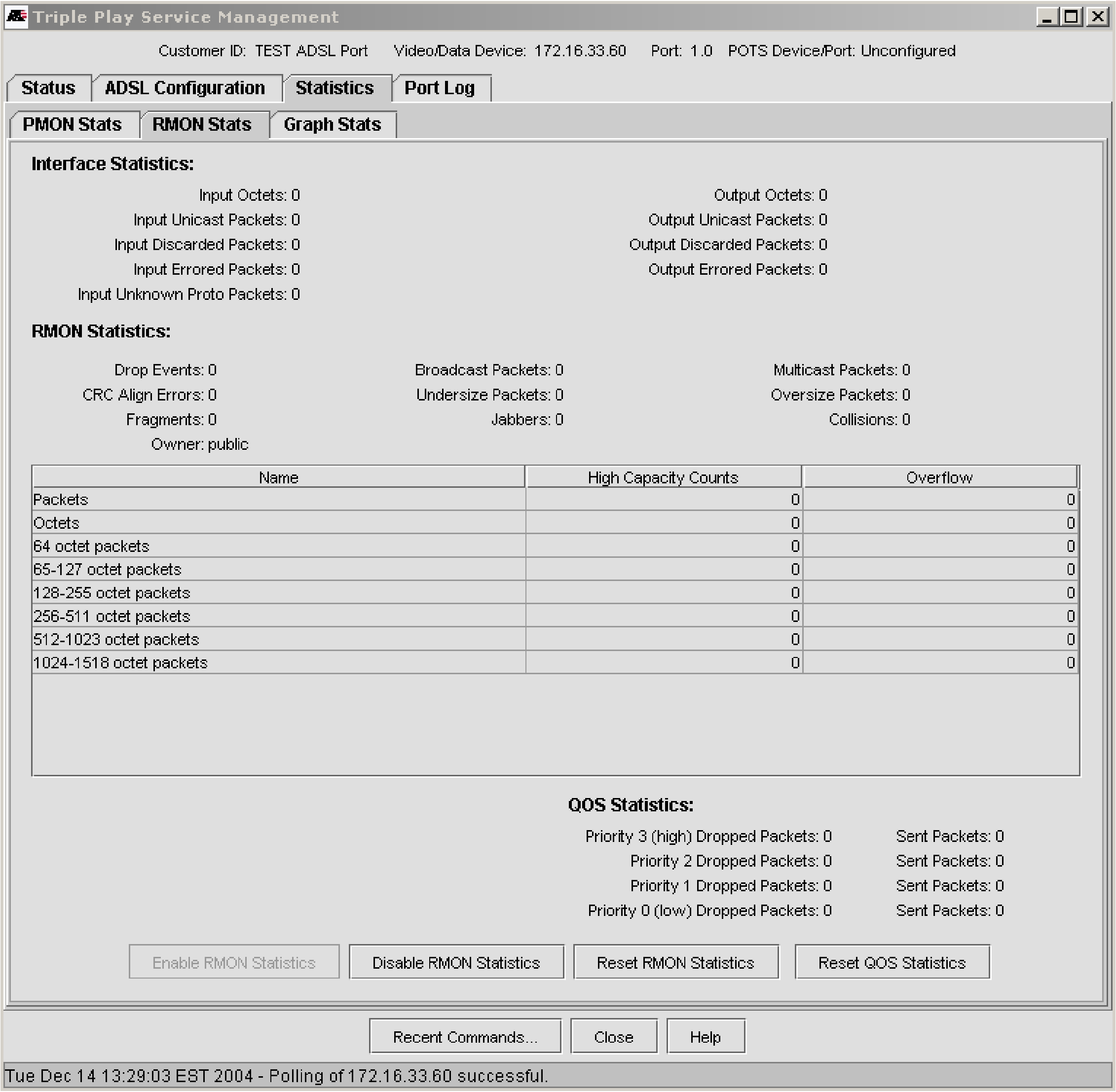
14.15.13 ADSL Statistics Tab - RMON Stats

RMON Statistics deal with packet flows and highlight errors as well as overflows of packets.

The QOS Statistics are counters for each priority queue that allow the user to see the ratio of sent versus dropped packets. These are cumulative and so produce no management logs.

These counters can be reset to 0 by selecting **Reset QOS Statistics**.

Refer to the *Software Reference for iMAP Series Switches* for details about these counters.



Customer ID: TEST ADSL Port Video/Data Device: 172.16.33.60 Port: 1.0 POTS Device/Port: Unconfigured

Interface Statistics:

Input Octets: 0	Output Octets: 0
Input Unicast Packets: 0	Output Unicast Packets: 0
Input Discarded Packets: 0	Output Discarded Packets: 0
Input Errored Packets: 0	Output Errored Packets: 0
Input Unknown Proto Packets: 0	

RMON Statistics:

Drop Events: 0	Broadcast Packets: 0	Multicast Packets: 0
CRC Align Errors: 0	Undersize Packets: 0	Oversize Packets: 0
Fragments: 0	Jabbers: 0	Collisions: 0
Owner: public		

Name	High Capacity Counts	Overflow
Packets	0	0
Octets	0	0
64 octet packets	0	0
65-127 octet packets	0	0
128-255 octet packets	0	0
256-511 octet packets	0	0
512-1023 octet packets	0	0
1024-1518 octet packets	0	0

QOS Statistics:

Priority 3 (high) Dropped Packets: 0	Sent Packets: 0
Priority 2 Dropped Packets: 0	Sent Packets: 0
Priority 1 Dropped Packets: 0	Sent Packets: 0
Priority 0 (low) Dropped Packets: 0	Sent Packets: 0

Tue Dec 14 13:29:03 EST 2004 - Polling of 172.16.33.60 successful.

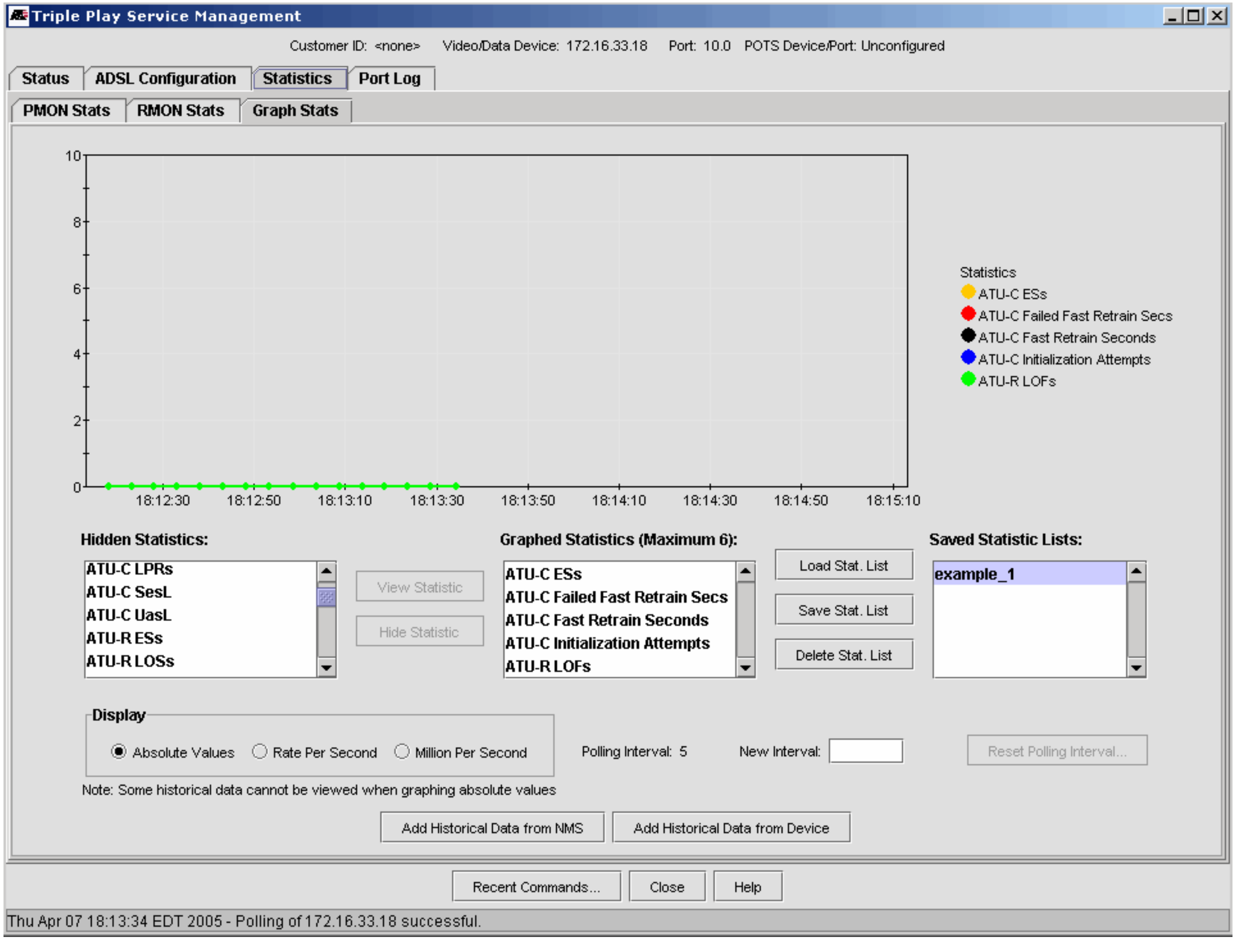
FIGURE 14-38 ADSL Statistics Form - RMON Stats Tab

TABLE 14-14 View Details Form, RMON Stats Tab

Field/Button	Description
Interface Statistics	Counts of input and output octets as well as errored input and output packets.
RMON Statistics	RMON error statistics
QOS Statistics	Shows the number of packets sent and dropped for each queue.
Enable RMON Statistics	If disabled, enables the statistics
Disable RMON Statistics	If enabled, disables the statistics
Reset RMON Statistics	Resets the RMON statistics to 0.
Reset QOS Statistics	Resets the QOS statistics to 0.

14.15.14 ADSL Statistics Tab - Graph Stats

Once the statistics have been enabled, they can be graphed both in real-time and for statistics that have been collected. The polling interval (in seconds) can be changed, and up to six statistics (each shown in a different color) can be shown at once, as shown in Figure 14-39.



Triple Play Service Management

Customer ID: <none> Video/Data Device: 172.16.33.18 Port: 10.0 POTS Device/Port: Unconfigured

Statistics
- ● ATU-C ESs
- ● ATU-C Failed Fast Retrain Secs
- ● ATU-C Fast Retrain Seconds
- ● ATU-C Initialization Attempts
- ● ATU-R LOFs

Hidden Statistics:
- ATU-C LPRs
- ATU-C SesL
- ATU-C UasL
- ATU-R ESs
- ATU-R LOSs

Graphed Statistics (Maximum 6):
- ATU-C ESs
- ATU-C Failed Fast Retrain Secs
- ATU-C Fast Retrain Seconds
- ATU-C Initialization Attempts
- ATU-R LOFs

Saved Statistic Lists:
- example_1

Display

● Absolute Values ○ Rate Per Second ○ Million Per Second

Polling Interval: 5 New Interval:

Note: Some historical data cannot be viewed when graphing absolute values

Reset Polling Interval...
Add Historical Data from NMS
Add Historical Data from Device
Recent Commands...
Close
Help

Thu Apr 07 18:13:34 EDT 2005 - Polling of 172.16.33.18 successful.

FIGURE 14-39 ADSL Statistics Form - Graph Stats Tab

Table 14-15 lists the buttons and fields available.

TABLE 14-15 ADSL Statistics Form - Graph Stats Tab

Field/Button	Description
Hidden Statistics	These are all the ATU-C and ATU-R statistics; form this set the ones to display are chosen.
Graphed Statistics	These are the ATU-C and ATU-R statistics that are currently displayed.
Polling Interval	This is the current polling interval, in seconds.
New Interval	This is used when changing the polling interval. When a new one is entered, the Reset Polling Interval Button is enabled, to allow the interval to be changed.
Add Historical Data from NMS	Include ADSL data that has been previously saved on the NMS
Add Historical Data from Device	Include ADSL data that has been previously saved from the historical data (buckets) of the device
Save Stat. List	Take a snapshot of the statistics chosen. A window appears to input a name.

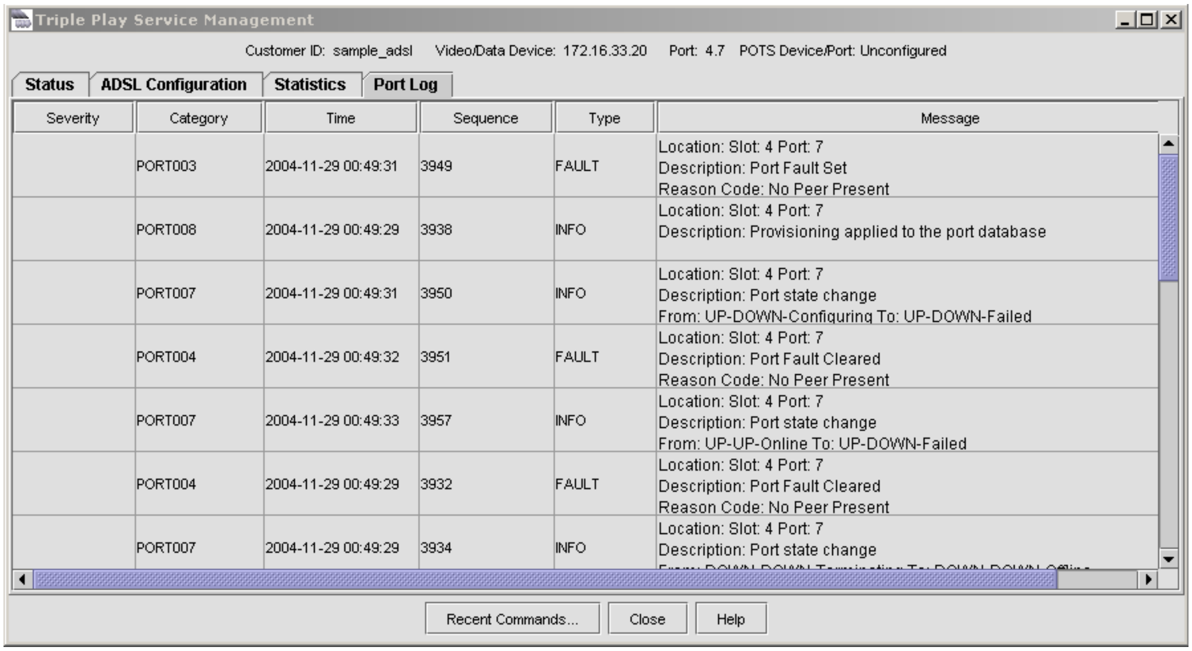
TABLE 14-15 ADSL Statistics Form - Graph Stats Tab (Continued)

Field/Button	Description
Load Stat. List	Load a previously saved statistic list
Delete Stat. List	Delete a statistic list that is chosen in the Saved Statistics List panel

14.15.15 ADSL Port - Port Log Tab)

Selecting the **Port Log** tab invokes a table that lists all the port-related management logs that have been generated. Refer to Figure 14-40.

For a description of management logs and the meaning of fields, refer to the iMAP Log / Troubleshooting Manual.



Customer ID: sample_adsl Video/Data Device: 172.16.33.20 Port: 4.7 POTS Device/Port: Unconfigured

Severity	Category	Time	Sequence	Type	Message
	PORT003	2004-11-29 00:49:31	3949	FAULT	Location: Slot: 4 Port: 7 Description: Port Fault Set Reason Code: No Peer Present
	PORT008	2004-11-29 00:49:29	3938	INFO	Location: Slot: 4 Port: 7 Description: Provisioning applied to the port database
	PORT007	2004-11-29 00:49:31	3950	INFO	Location: Slot: 4 Port: 7 Description: Port state change From: UP-DOWN-Configuring To: UP-DOWN-Failed
	PORT004	2004-11-29 00:49:32	3951	FAULT	Location: Slot: 4 Port: 7 Description: Port Fault Cleared Reason Code: No Peer Present
	PORT007	2004-11-29 00:49:33	3957	INFO	Location: Slot: 4 Port: 7 Description: Port state change From: UP-UP-Online To: UP-DOWN-Failed
	PORT004	2004-11-29 00:49:29	3932	FAULT	Location: Slot: 4 Port: 7 Description: Port Fault Cleared Reason Code: No Peer Present
	PORT007	2004-11-29 00:49:29	3934	INFO	Location: Slot: 4 Port: 7 Description: Port state change From: DOWN-DOWN-Terminating To: DOWN-DOWN-Offline

FIGURE 14-40 View Details Form (ADSL Port Log Tab)

14.16 SHDSL Port Management Form

Many of the SHDSL forms are similar to the ADSL forms. This subsection will focus on the differences; if forms or fields are the same, there is a reference to the appropriate ADSL subsection.

Note: There are changes to the GUIs if the SHDSL card is in Bonded (4-wire) mode.

Caution: Also, the card must be disabled when changing from 2-wire to 4-wire or vice-versa, so all provisioning information (i.e. Triple Play) is lost and must be re-provisioned.

14.16.1 SHDSL Port (Status Tab)

This tab is essentially the same as the ADSL Status tab, with the Video/Data Port, Voice, and Alerts panels. Since SHDSL is a high-speed data application, only the Voice/Data Port panel has information.

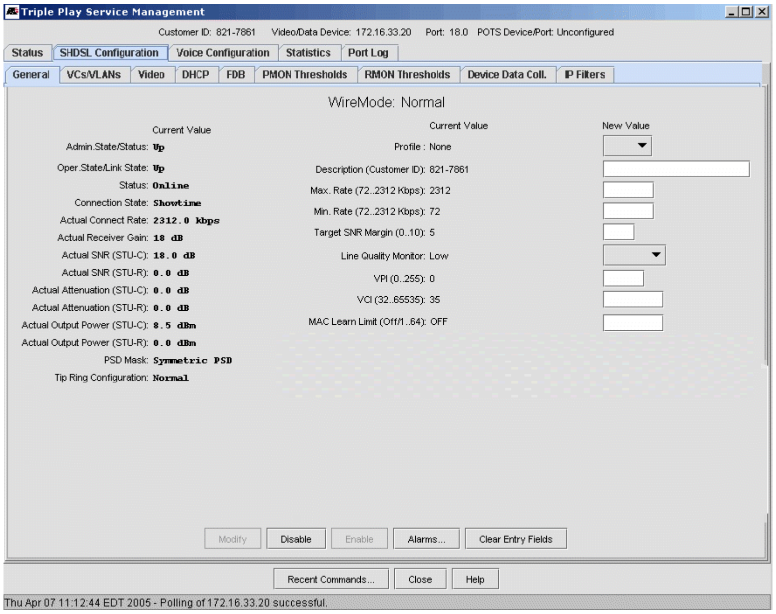
14.16.2 SHDSL Configuration Tab - Overview

The SHDSL Configuration tab has the following forms:

- General

- VCs/VLANs
- Video
- DHCP
- FDB
- PMON Thresholds
- Device Data Collection
- IP Filters

14.16.3 SHDSL Configuration Tab - General



Customer ID: 821-7861 Video/Data Device: 172.16.33.20 Port: 18.0 POTS Device/Port: Unconfigured

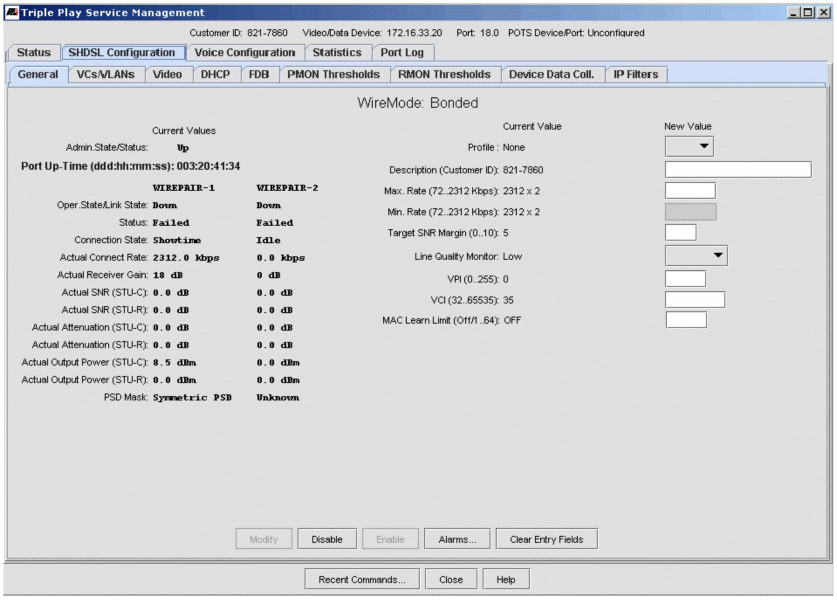
WireMode: Normal

	Current Value
Admin.State/Status:	Up
Oper.State/Link State:	Up
Status:	Online
Connection State:	Showtime
Actual Connect Rate:	2312.0 kbps
Actual Receiver Gain:	18 dB
Actual SNR (STU-C):	18.0 dB
Actual SNR (STU-R):	0.0 dB
Actual Attenuation (STU-C):	0.0 dB
Actual Attenuation (STU-R):	0.0 dB
Actual Output Power (STU-C):	8.5 dBm
Actual Output Power (STU-R):	0.0 dBm
PSD Mask:	Symmetric PSD
Tip Ring Configuration:	Normal

	Current Value	New Value
Profile :	None	
Description (Customer ID):	821-7861	
Max. Rate (72..2312 Kbps):	2312	
Min. Rate (72..2312 Kbps):	72	
Target SNR Margin (0..10):	5	
Line Quality Monitor:	Low	
VPI (0..255):	0	
VCI (32..65535):	35	
MAC Learn Limit (Off/1..64):	OFF	

Thu Apr 07 11:12:44 EDT 2005 - Polling of 172.16.33.20 successful.

FIGURE 14-41 SHDSL Configuration Tab - General - Normal



Customer ID: 821-7860 Video/Data Device: 172.16.33.20 Port: 18.0 POTS Device/Port: Unconfigured

WireMode: Bonded

	Current Values	
Admin.State/Status:	Up	
Port Up-Time (ddd:hh:mm:ss): 003:20:41:34		
	WIREPAIR-1	WIREPAIR-2
Oper.State/Link State:	Down	Down
Status:	Failed	Failed
Connection State:	Showtime	Idle
Actual Connect Rate:	2312.0 kbps	0.0 kbps
Actual Receiver Gain:	18 dB	0 dB
Actual SNR (STU-C):	0.0 dB	0.0 dB
Actual SNR (STU-R):	0.0 dB	0.0 dB
Actual Attenuation (STU-C):	0.0 dB	0.0 dB
Actual Attenuation (STU-R):	0.0 dB	0.0 dB
Actual Output Power (STU-C):	8.5 dBm	0.0 dBm
Actual Output Power (STU-R):	0.0 dBm	0.0 dBm
PSD Mask:	Symmetric PSD	Unknown

	Current Value	New Value
Profile :	None	
Description (Customer ID):	821-7860	
Max. Rate (72..2312 Kbps):	2312 x 2	
Min. Rate (72..2312 Kbps):	2312 x 2	
Target SNR Margin (0..10):	5	
Line Quality Monitor:	Low	
VPI (0..255):	0	
VCI (32..65535):	35	
MAC Learn Limit (Off/1..64):	OFF	

FIGURE 14-42 SHDSL Configuration Tab - General - Bonded

TABLE 14-16 SHDSL Configuration Tab - General

Field/Button	Description
WireMode	Whether the port is 2-wire (Normal) or 4-wire (Bonded)
Admin. State/Status	The Administrative State can be controlled and determines the Operational State. For a bonded pair, the Admin State determines the Oper. State of both wire pairs.
Oper. State/Link State	The ability of the port to provide service. The Administrative State must be up and then the system determines if the port can provide service. It is possible, in a bonded configuration, that one wire pair will be Up while the other pair is Down. The line can still provide service, although at a lower rate. The user should check for events/logs and fix the problem.
Port Up-Time	Amount of time the physical interface has been in the UP-UP-Online state.
Status	The status of the port that follows form the Administrative State and Operational State. For meanings, refer to the *Software Reference for iMAP Series Switches*. - ONLINE - IN TEST - FAILED - OFFLINE - DEPENDENCY - DEGRADED - NOT INSTALLED - INITIALIZATION REQUIRED - TERMINATING
Wire Mode	Normal (2-wire) or Bonded (4-wire)
Connection State	The connection state, such as Idle or Showtime
Actual Connect Rate	The data rate that was actually attained.

TABLE 14-16 SHDSL Configuration Tab - General

Field/Button	Description
Actual Receiver Gain	Receiver Gain in db.
Actual SNR (STU-C, STU-R)	The signal-noise ratios that were actually attained.
Actual Attenuation (STU-C, STU-R)	The attenutation that was actually attained.
Actual Output Power (STU-C, STU-R)	The power outputs that were actually attained
PSD Mask	PSD (Power Spectral Density) is a measure of how power in a signal changes over frequency, and is expressed in dBms per Hz bandwidth. Values for SHDSL16 are: Symmetric Region 1 (Annex-A) Symmetric Region 2 (Annex-B)
Tip Ring Configuration	Values are Normal and Reversed
Profile	Which profile is being used (AutoProv or none, which uses default values).
Description (Customer ID)	An ID that can be given to uniquely identify the port. In most cases, the subscriber's telephone number is used.
Max. Rate	The maximum upstream rate that is provisioned.
Min. Rate	The minimum upstream rate that is provisioned.
Target SNR Margin	Specifies the target signal-to-noise ratio (in dB) to achieve on an ADSL port.
Line Quality Monitor	Specifies the ADSL line type as per ITU G.992. Allowed values are FAST and INTERLEAVE, although FAST is not allowed if the MODE is GLITE. Refer to the iMAP User's Guide, Section 4.
VPI	Specifies the value for the ATM virtual path identifier on an ADSL port. Refer to the iMAP User's Guide, Section 4.
VCI	Specifies the value for the ATM virtual channel identifier on an ADSL port. Refer to the iMAP User's Guide, Section 4.
MAC Learn Limit	Depending on feature provisioning, the number of MAC addresses that can be learned (or Off)
Modify	Enabled when a value in New Value field has been entered, modifies the attributes according to the updated values.There is an error message if a value is invalid.
Enable	Enabled if the port is in an Administrative State of DOWN, enables the port and so brings the Administrative State to UP. If possible (for example, the ADSL card must be enabled), the Operational State will change to UP.
Disable	Enabled if the port is in an Administrative State of UP, disables the port and so brings the Administrative State to DOWN. The Operational State will also change to DOWN.
Alarms	Invokes the Alarm table of the Fault Management Object.

14.16.4 SHDSL Configuration Tab - VCs/VLANs

Note: *The ADSL16 and ADSL8S cards allow up to four VCs to be configured per port, while the ADSL24 card allows only one VC per port. The ADSL24A/B card supports 4 VCs.*

Refer to "ADSL Configuration Tab - VCs/VLANs" on page 434.

14.16.5 SHDSL Configuration Tab - Video Tab

This screen has the same attributes as for ADSL. Refer to "Video Tab" on page 485

14.16.6 SHDSL Configuration Tab - DHCP Tab

Refer to "DHCP Tab" on page 485.

14.16.7 SHDSL Configuration Tab - FDB Tab

Refer to "FDB Tab" on page 485.

14.16.8 SHDSL Configuration Tab - PMON Thresholds

This form shows (any) threshold values for the STU-C/R statistics.

Note: *The thresholds are set for both the STU-C and STU-R at the same time and cannot be set separately.*

14.16.9 SHDSL Configuration Tab - Device Data Collection

The Device Data Coll form has the same functions as the ADSL form as explained in "ADSL Configuration Tab - Device Data Collection Tab" on page 436

14.16.10 SHDSL Configuration Tab - IP Filters

The IP Filters form has the same functions as the ADSL form as explained in "ADSL Configuration Tab - IP Filters" on page 437

14.16.11 SHDSL Statistics Tab - PMON Stats

The PMON Stats form is similar to the ADSL form except for the following:

- The statistics are the standard ones defined in RC3276. (STU-C and STU-R).
- There is no history of statistics (no previous day)
- If the port is bonded, each statistics column has Wire Pair-1 and Wire Pair-2 to show statistics for each pair.

14.16.12 SHDSL Statistics Tab - RMON Stats

The RMON Stats form has the same functions as the ADSL form as explained in "ADSL Statistics Tab - RMON Stats" on page 441. For a bonded pair, these statistics tread the bonded pair as one wire.

14.16.13 SHDSL Statistics Tab - Graph Stats

The Stats Graph form has the same functions as the ADSL form as explained in "ADSL Statistics Tab - Graph Stats" on page 443. For a bonded pair, the STU-C and STU-R have WP-1 and WP-2 so the user can display these for each statistic.

14.16.14 SHDSL Statistics Tab - Port Log

The Port Log form has the same functions as the ADSL form as explained in "ADSL Port - Port Log Tab)" on page 444

14.17 Voice Port Management (Tabbed Form)

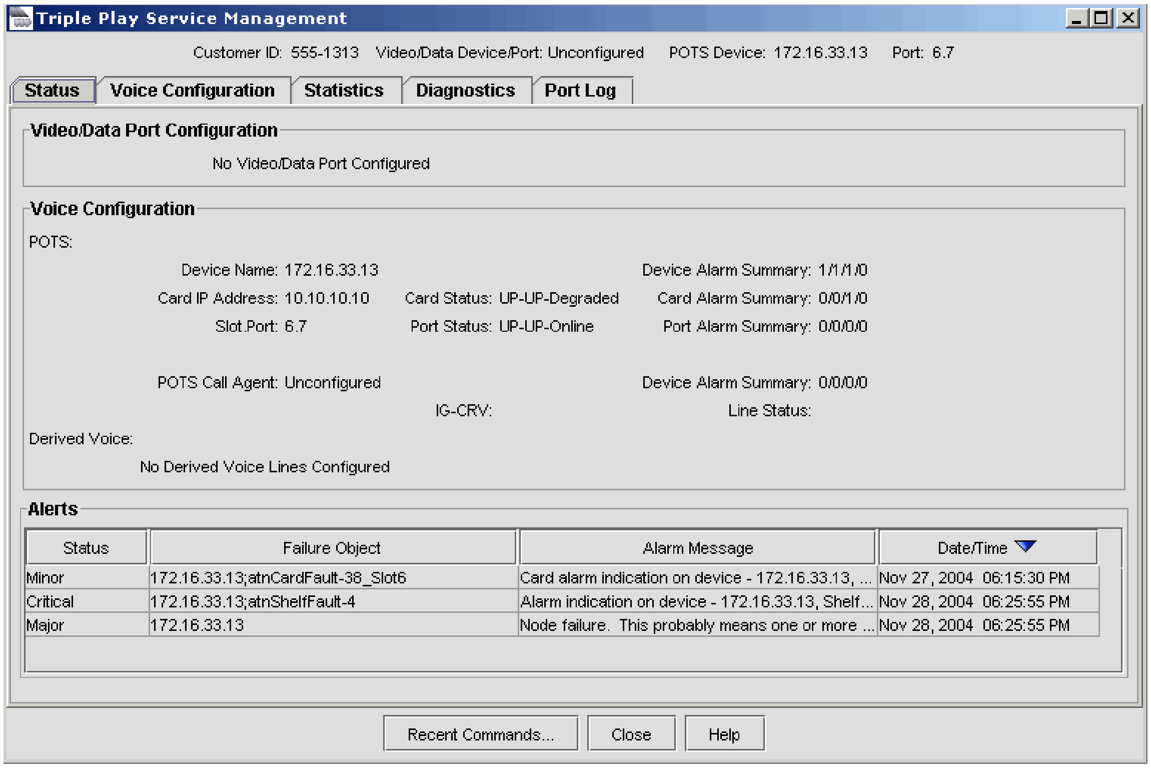
14.17.1 POTS24 Configuration Tab - Overview

When the POTS 24 is configured (as part of a customer configuration that includes analog voice), this service management from provides all the relevant data.

Note: *When an iMG/RG is configured for voice service using the GenBand, information about this configuration is shown in the Voice Configuration tab. Refer to Section 7.*

14.17.2 POTS24 Configuration Tab - Status

This form is similar to other port types, and lists the POTS attributes as well as Alerts



Customer ID: 555-1313 Video/Data Device/Port: Unconfigured POTS Device: 172.16.33.13 Port: 6.7

Video/Data Port Configuration

No Video/Data Port Configured

Voice Configuration

POTS:

Device Name: 172.16.33.13 Device Alarm Summary: 1/1/1/0

Card IP Address: 10.10.10.10 Card Status: UP-UP-Degraded Card Alarm Summary: 0/0/1/0

Slot.Port: 6.7 Port Status: UP-UP-Online Port Alarm Summary: 0/0/0/0

POTS Call Agent: Unconfigured Device Alarm Summary: 0/0/0/0

IG-CRV: Line Status:

Derived Voice:

No Derived Voice Lines Configured

Alerts

Status	Failure Object	Alarm Message	Date/Time ▼
Minor	172.16.33.13;atnCardFault-38_Slot6	Card alarm indication on device - 172.16.33.13, ...	Nov 27, 2004 06:15:30 PM
Critical	172.16.33.13;atnShelfFault-4	Alarm indication on device - 172.16.33.13, Shelf...	Nov 28, 2004 06:25:55 PM
Major	172.16.33.13	Node failure. This probably means one or more ...	Nov 28, 2004 06:25:55 PM

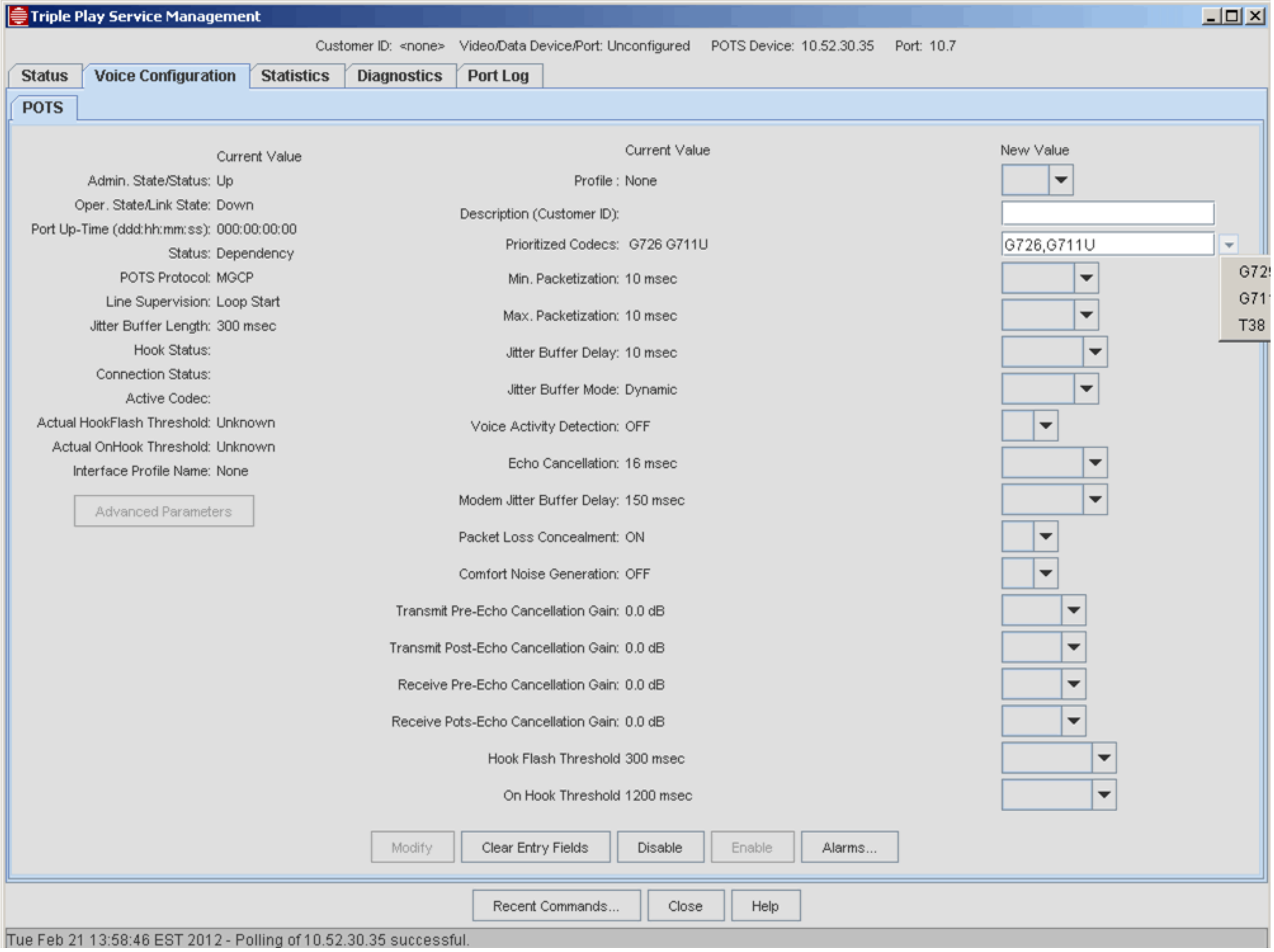
FIGURE 14-43 POTS24 Configuration Tab - Status

14.17.3 POTS24 Voice Configuration Tab - POTS

Each port on the POTS24 provides an analog interface to a physical customer loop. Configurable attributes for each line interface specify the capabilities of the line that affect analog waveform transmission and packetization of the analog waveform. Differences between the SIP versus MGCP protocol parameters are noted in the table below.

Note: *The Voice Configuration tab also shows information for the iMG/RG when the Derived Voice has been provisioned using the GenBand. Otherwise, there is the message "Derived voice gateway information is not available." This means that the NMS does not manage the device that provides the service.*

Caution: *Modification of these attributes requires the port to be disabled.*



Customer ID: <none> Video/Data Device/Port: Unconfigured POTS Device: 10.52.30.35 Port: 10.7

	Current Value
Admin. State/Status:	Up
Oper. State/Link State:	Down
Port Up-Time (ddd:hh:mm:ss):	000:00:00:00
Status:	Dependency
POTS Protocol:	MGCP
Line Supervision:	Loop Start
Jitter Buffer Length:	300 msec
Hook Status:	
Connection Status:	
Active Codec:	
Actual HookFlash Threshold:	Unknown
Actual OnHook Threshold:	Unknown
Interface Profile Name:	None

	Current Value	New Value
Profile :	None	
Description (Customer ID):		
Prioritized Codecs:	G726 G711U	G726,G711U
Min. Packetization:	10 msec	
Max. Packetization:	10 msec	
Jitter Buffer Delay:	10 msec	
Jitter Buffer Mode:	Dynamic	
Voice Activity Detection:	OFF	
Echo Cancellation:	16 msec	
Modem Jitter Buffer Delay:	150 msec	
Packet Loss Concealment:	ON	
Comfort Noise Generation:	OFF	
Transmit Pre-Echo Cancellation Gain:	0.0 dB	
Transmit Post-Echo Cancellation Gain:	0.0 dB	
Receive Pre-Echo Cancellation Gain:	0.0 dB	
Receive Pots-Echo Cancellation Gain:	0.0 dB	
Hook Flash Threshold	300 msec	
On Hook Threshold	1200 msec	

Tue Feb 21 13:58:46 EST 2012 - Polling of 10.52.30.35 successful.

FIGURE 14-44 Example POTS24 Voice Configuration Tab - POTS (SIP Protocol)

TABLE 14-17 POTS24 Voice Configuration Tab - POTS

Field/Button	Description
Admin. State/Status:	The Administrative State can be controlled and determines the Operational State.
Oper. State/Link State:	The ability of the port to provide service. The Administrative State must be up and then the system determines if the port can provide service.
Port Up-Time	Amount of time the physical interface has been in the UP-UP-Online state.

TABLE 14-17 POTS24 Voice Configuration Tab - POTS

Field/Button	Description
Status:	The status of the port that follows form the Administrative State and Operational State. For meanings, refer to the *Software Reference for iMAP Series Switches*. - ONLINE - IN TEST - FAILED - OFFLINE - DEPENDENCY - DEGRADED - NOT INSTALLED - INITIALIZATION REQUIRED - TERMINATING
POTS Protocol	Whether the card is using MGCP or SIP protocol
Profile:	Profile used that pre-populates many of the port attributes.
Description (Customer ID):	Customer ID for the port. Refer to "Naming Convention for Customer IDs (Triple Play Form)" on page 780.
Prioritized Codecs	Specifies the Codec capabilities advertised to the Call Agent: - PCMU: G.711 mu law (specified in CCITT/ITU-T recommendation G.711) - G726-32: CCITT/ITU-T recommendation G.726 - T38 - Use this mode to digitize the media for reliable transmission over IP networks - All: all of the above
Min. Packetization:	The minimum number of milliseconds of voice data that can be encoded in a data packet. This value is advertised to the Call Agent. The default is **20** msec. *Note: To support Call Waiting with Caller ID, this attribute should be set to 10 milliseconds.*
Max. Packetization	The maximum number of milliseconds of voice data that can be encoded in a data packet. This value is advertised to the Call Agent. The default is **20** msec. *Note: To support Call Waiting with Caller ID, this attribute should be set to 10 milliseconds*
Jitter Buffer Delay:	Used with jitter buffering, this is the amount of time that the first packet is delayed. This delay is then used to smooth out jitter on subsequent arrivals. The default is **30** msec
Jitter Buffer Mode:	The jitter buffer mode. A jitter buffer is used to compensate for the jitter in packet arrival and out-of-order packets. A large jitter buffer causes increase in the delay and decreases the packet loss. A small jitter buffer decreases the delay but increases the packet loss. **DYNAMIC** - This mode minimizes delays and is the default.
Voice Activity Detection:	Specifies whether to advertise Voice Activity Detection (VAD) capability to the Call Agent. VAD is used for silence suppression, and will reduce the transmission rate during inactive speech periods while maintaining an acceptable level of output quality. **ON**: VAD is supported. This is the default
Echo Cancellation:	Echo Cancellation in ms for period capability is advertised to the Call Agent.

TABLE 14-17 POTS24 Voice Configuration Tab - POTS

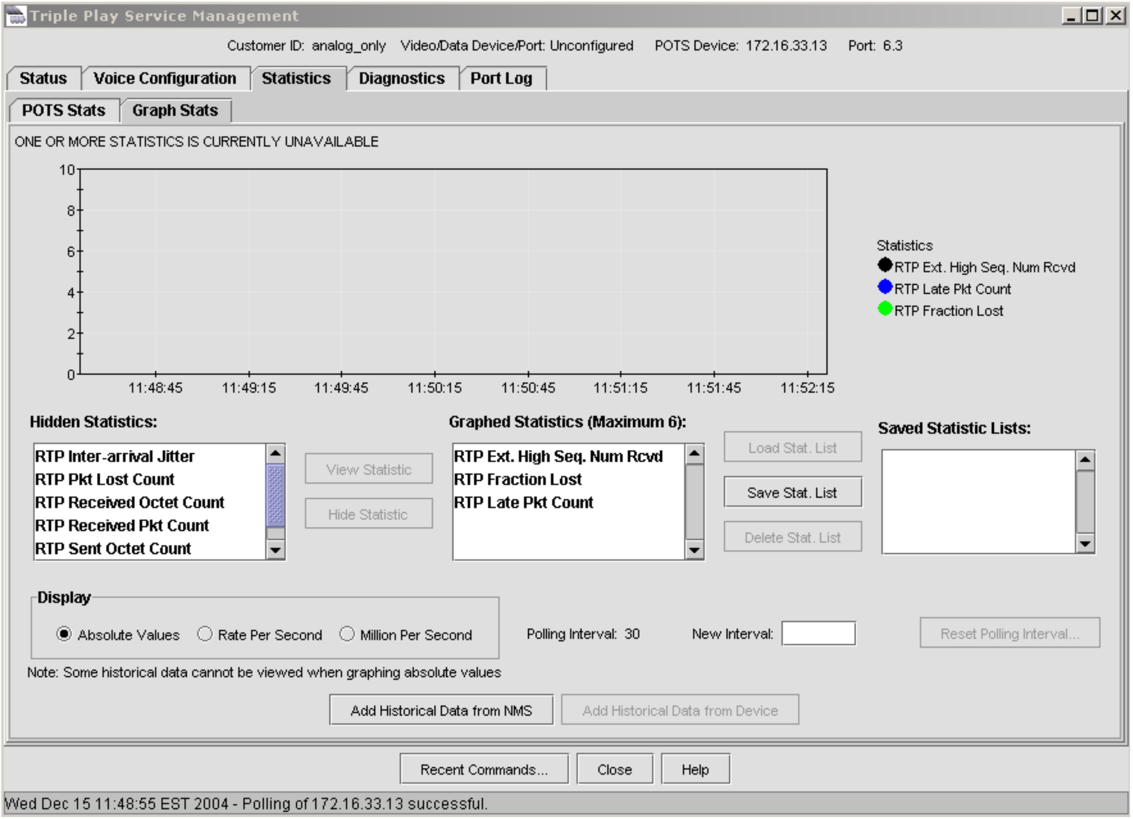
Field/Button	Description
Modem Jitter Buffer Delay	Used with jitter buffering, this is the amount of time that the first packet is delayed. *Note: The default in release 8.0 was changed from 30ms to 10ms*
Packet Loss Concealment:	Specifies whether Packet Loss Concealment is enabled. Packet Loss Concealment is a technique used on the receive side of the voice packet stream to mask the effects of lost or discarded packets. If not used, users may report difficulty in understanding speech due to short gaps. Default is **ON**.
Comfort Noise Generation:	Specifies whether or not to generate Comfort Noise (RFC 3389). To generate background noise to fill silent gaps during calls if voice activity detection (VAD) is activated; **The parameter should be ON**.
Transmit Pre-Echo Cancellation Gain	The gain applied on the transmit side before echo cancellation is applied. Values are:-9.0 to +3.0
Transmit Post-Echo Cancellation Gain	The gain applied on the transmit side after echo cancellation is applied. Values are:-9.0 to +3.0
Receive Pre-Echo Cancellation Gain	The gain applied on the receive side before echo cancellation is applied. Values are:-9.0 to +3.
Sip User Name	This is used to identify the user and is usually a DN.
Sip Password	Used with the User Name to authenticate an endpoint to a server.
Sip Digit String	Has rules for how digits are parsed.
Sip Display Name	Name that appears on the display of the SIP-enabled VoIP device.
Modify	Enabled when a field has been entered or changed.
Disable	Disables the port, which must be done before attributes can be changed
Enable	Enables the port
Alarms	Brings up the Alarm view for the selected port.
Clear Entry Fields	Clears the writable fields of any values.

14.17.4 POTS24 Statistics Tab - POTS Stats

This tab lists the RTP statistics for the card. Refer to the *Software Reference for iMAP Series Switches* for details.

14.17.5 POTS24 Statistics Tab - Graphs Stats

This window makes a graph of selected statistics and displays them with varying attributes. Refer to the following figure and table.



Customer ID: analog_only Video/Data Device/Port: Unconfigured POTS Device: 172.16.33.13 Port: 6.3

ONE OR MORE STATISTICS IS CURRENTLY UNAVAILABLE

Hidden Statistics:

RTP Inter-arrival Jitter
RTP Pkt Lost Count
RTP Received Octet Count
RTP Received Pkt Count
RTP Sent Octet Count

Graphed Statistics (Maximum 6):

RTP Ext. High Seq. Num Rcvd
RTP Fraction Lost
RTP Late Pkt Count

Saved Statistic Lists:

Display

● Absolute Values ○ Rate Per Second ○ Million Per Second

Polling Interval: 30 New Interval:

Note: Some historical data cannot be viewed when graphing absolute values

Wed Dec 15 11:48:55 EST 2004 - Polling of 172.16.33.13 successful.

FIGURE 14-45 POTS24 Statistics Tab - Graphs Stats

TABLE 14-18 POTS24 Statistics Tab - Graphs Stats

Field/Button	Description
Hidden Statistics:	Statistics not added to the resulting graph
View Statistic:	Enabled when a statistic is chosen form Hidden Statistics, clicking this button adds it to the graph/
Hide Statistic:	Enabled when a statistic is chosen form Graphed Statistics, clicking this button deletes it from the graph/
Display	The attribute that controls the display: - Absolute Values - Rate Per Second - Million Per Second
Polling Interval:	Current Polling Interval in seconds
New Interval:	Sets a new interval for polling. This is set with the **Reset Polling Interval** button.
Enable Statistics	Enables the graph for the statistics chosen.
Disable Statistics:	Disables the graph
Add Historical Data from NMS:	Adds the data collected previously from NMS port management

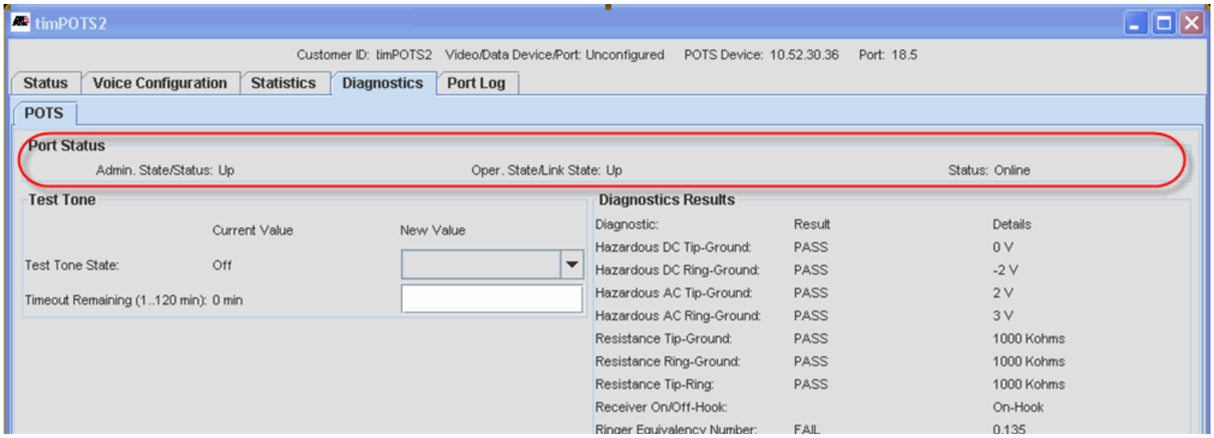
14.17.6 POTS24 Diagnostics Tab - POTS

This form allows the user to run a set of diagnostics on the port interface. Refer to the following figure and table.

- T/G, R/G, T/R capacitance measurements added to suite of measurements from "DIAGNOSE INTERFACE" function
- New CLI command for generation of a Toll grade defined metallic tone used for T/R identification

Following are the changes to the Diagnostics tab to support this feature.

A panel across the top on the Diagnostics tab shows port state information that applies to both Test Tone and Diagnostics functionality.



Customer ID: timPOTS2 Video/Data Device/Port: Unconfigured POTS Device: 10.52.30.36 Port: 18.5

Port Status

Admin. State/Status: Up Oper. State/Link State: Up Status: Online

Test Tone

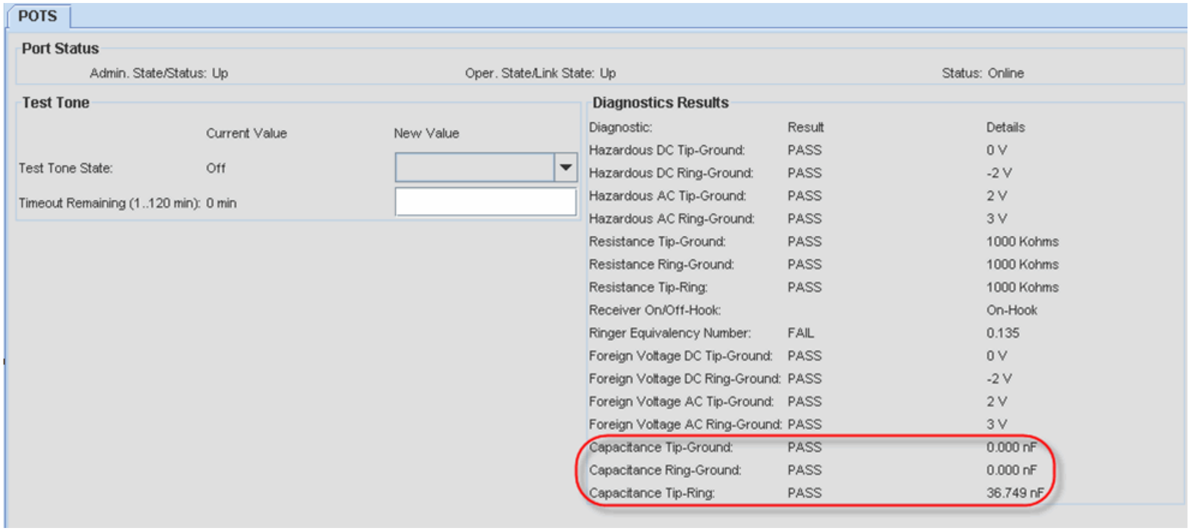
	Current Value	New Value
Test Tone State:	Off	
Timeout Remaining (1..120 min):	0 min	

Diagnostics Results

Diagnostic:	Result	Details
Hazardous DC Tip-Ground:	PASS	0 V
Hazardous DC Ring-Ground:	PASS	-2 V
Hazardous AC Tip-Ground:	PASS	2 V
Hazardous AC Ring-Ground:	PASS	3 V
Resistance Tip-Ground:	PASS	1000 Kohms
Resistance Ring-Ground:	PASS	1000 Kohms
Resistance Tip-Ring:	PASS	1000 Kohms
Receiver On/Off-Hook:		On-Hook
Ringer Equivalency Number:	FAIL	0.135

FIGURE 14-46 POTS24 Diagnostics Tab - Port Status

New rows have been added to the Diagnostics Results table to display the Capacitance test results and details/values.



Port Status

Admin. State/Status: Up Oper. State/Link State: Up Status: Online

Test Tone

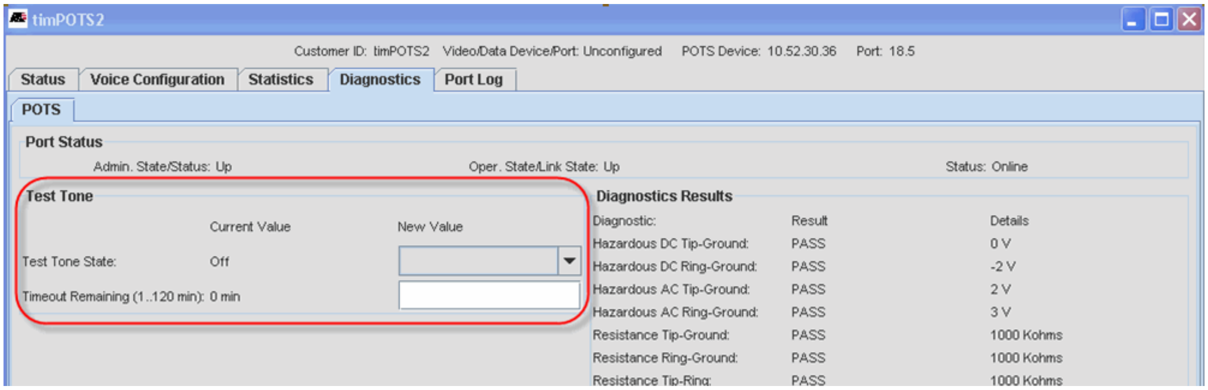
	Current Value	New Value
Test Tone State:	Off	
Timeout Remaining (1..120 min):	0 min	

Diagnostics Results

Diagnostic:	Result	Details
Hazardous DC Tip-Ground:	PASS	0 V
Hazardous DC Ring-Ground:	PASS	-2 V
Hazardous AC Tip-Ground:	PASS	2 V
Hazardous AC Ring-Ground:	PASS	3 V
Resistance Tip-Ground:	PASS	1000 Kohms
Resistance Ring-Ground:	PASS	1000 Kohms
Resistance Tip-Ring:	PASS	1000 Kohms
Receiver On/Off-Hook:		On-Hook
Ringer Equivalency Number:	FAIL	0.135
Foreign Voltage DC Tip-Ground:	PASS	0 V
Foreign Voltage DC Ring-Ground:	PASS	-2 V
Foreign Voltage AC Tip-Ground:	PASS	2 V
Foreign Voltage AC Ring-Ground:	PASS	3 V
Capacitance Tip-Ground:	PASS	0.000 nF
Capacitance Ring-Ground:	PASS	0.000 nF
Capacitance Tip-Ring:	PASS	36.749 nF

FIGURE 14-47 POTS24 Diagnostics Tab - Capacitance Test Results

A new panel has been added specifically for handling Test Tone information



Customer ID: timPOTS2 Video/Data Device/Port: Unconfigured POTS Device: 10.52.30.36 Port: 18.5

Port Status

Admin. State/Status: Up Oper. State/Link State: Up Status: Online

Test Tone

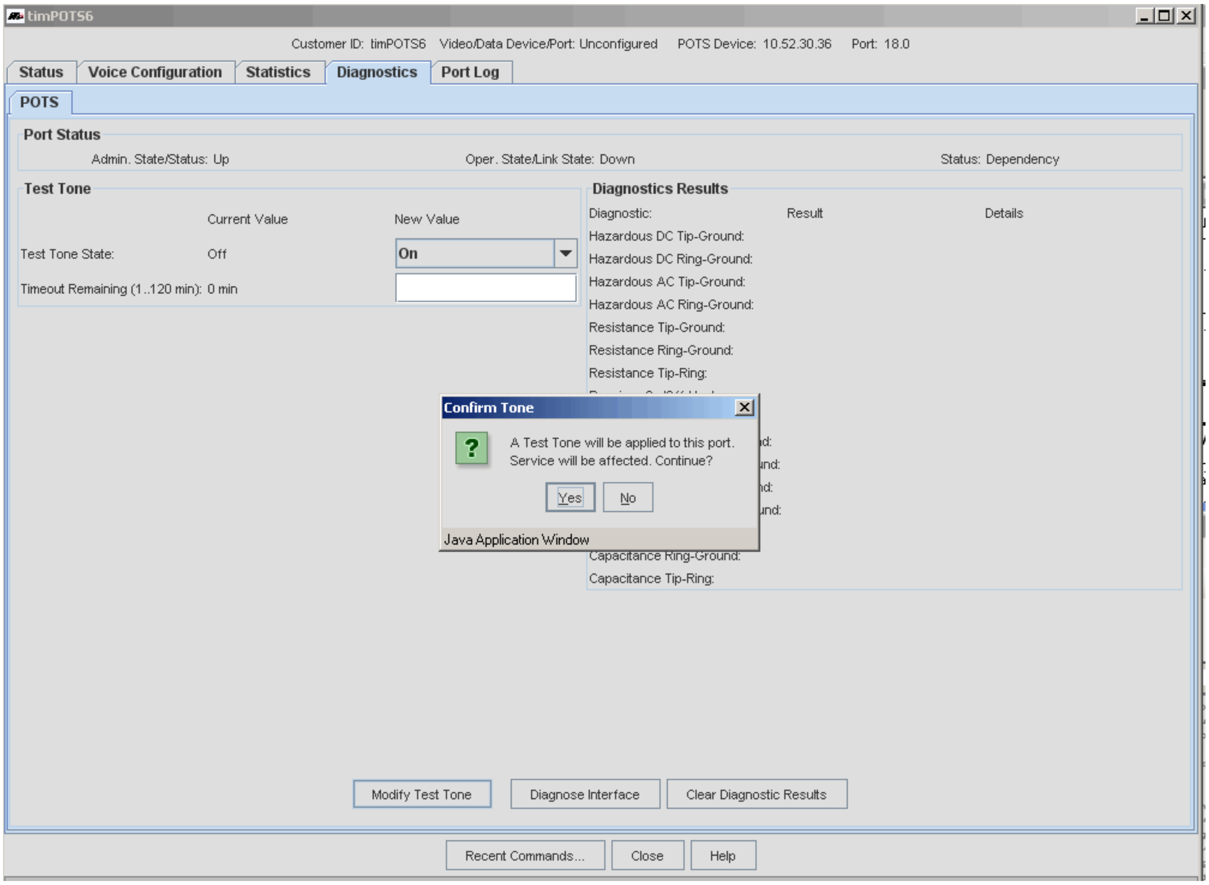
	Current Value	New Value
Test Tone State:	Off	
Timeout Remaining (1..120 min):	0 min	

Diagnostics Results

Diagnostic:	Result	Details
Hazardous DC Tip-Ground:	PASS	0 V
Hazardous DC Ring-Ground:	PASS	-2 V
Hazardous AC Tip-Ground:	PASS	2 V
Hazardous AC Ring-Ground:	PASS	3 V
Resistance Tip-Ground:	PASS	1000 Kohms
Resistance Ring-Ground:	PASS	1000 Kohms
Resistance Tip-Ring:	PASS	1000 Kohms

FIGURE 14-48 POTS24 Diagnostics Tab - Test Tone Information

The button Modify Test Tone is used when modifying the Test Tone information. Note that when turing the Test Tone status to On and making changes to the Time-out, there is a warning about service. Refer to the following figure.



Customer ID: timPOTS6 Video/Data Device/Port: Unconfigured POTS Device: 10.52.30.36 Port: 18.0

Port Status

Admin. State/Status: Up Oper. State/Link State: Down Status: Dependency

Test Tone

	Current Value	New Value
Test Tone State:	Off	On
Timeout Remaining (1..120 min):	0 min	

Diagnostics Results

Diagnostic:	Result	Details
Hazardous DC Tip-Ground:		
Hazardous DC Ring-Ground:		
Hazardous AC Tip-Ground:		
Hazardous AC Ring-Ground:		
Resistance Tip-Ground:		
Resistance Ring-Ground:		
Resistance Tip-Ring:		
Capacitance Ring-Ground:		
Capacitance Tip-Ring:		

Confirm Tone

A Test Tone will be applied to this port. Service will be affected. Continue?

Yes No

Java Application Window

FIGURE 14-49 Modifying Test Tone Information

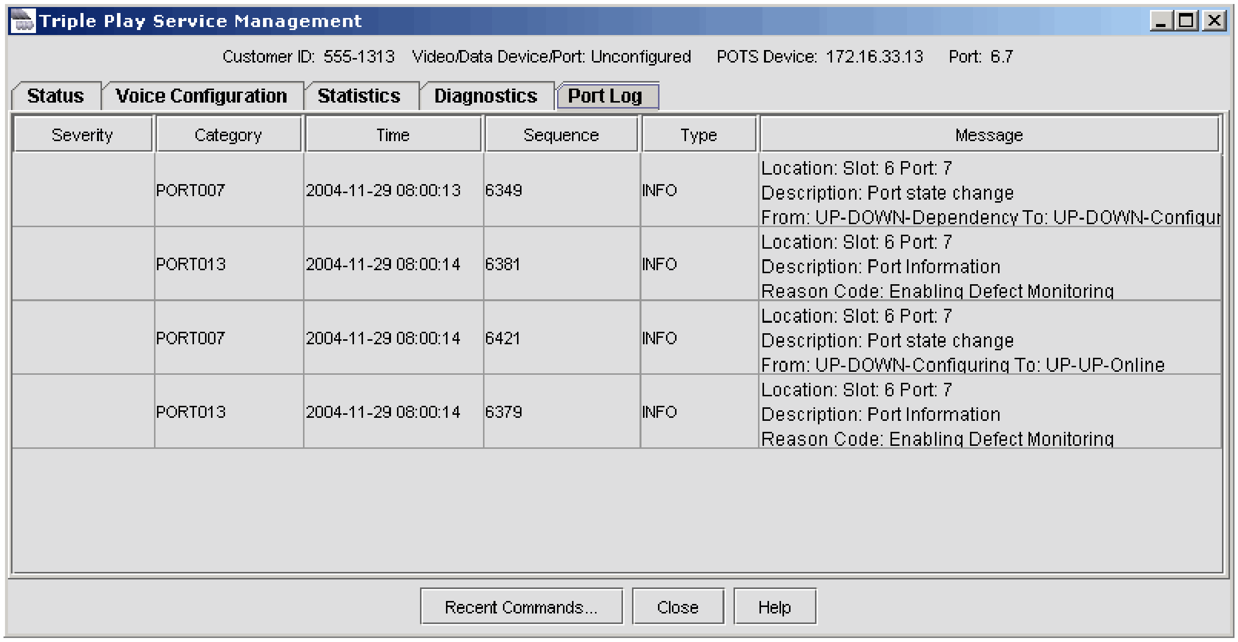
TABLE 14-19 POTS24 Diagnostics Tab - POTS

Field/Button	Description
Diagnostic Results	Refer to the *Software Reference for iMAP Series Switches* for an explanation of these test functions.
Diagnostic: Result	For each test, there is a Result field that says PASS or FAIL and a Details field that gives the specific test result.
Modify Test Tone	For making changes to Test Tone settings. When changing state to ON, there is a service warning.
Diagnose Interface	This runs the diagnostics listed and gives the test results
Clear Diagnostic Results	Clears any previous diagnostic results

14.17.7 POTS Port (Port Log Tab)

Selecting the **Port Log** tab invokes a table that lists all the port-related management logs that have been generated. Refer to Figure 14-50. This window has the same columns as the ADSL Port Management window for Port Log.

For a description of management logs and the meaning of fields, refer to the iMAP Log / Troubleshooting Manual.



Customer ID: 555-1313 Video/Data Device/Port: Unconfigured POTS Device: 172.16.33.13 Port: 6.7

Severity	Category	Time	Sequence	Type	Message
	PORT007	2004-11-29 08:00:13	6349	INFO	Location: Slot: 6 Port: 7 Description: Port state change From: UP-DOWN-Dependency To: UP-DOWN-Configur
	PORT013	2004-11-29 08:00:14	6381	INFO	Location: Slot: 6 Port: 7 Description: Port Information Reason Code: Enabling Defect Monitoring
	PORT007	2004-11-29 08:00:14	6421	INFO	Location: Slot: 6 Port: 7 Description: Port state change From: UP-DOWN-Configuring To: UP-UP-Online
	PORT013	2004-11-29 08:00:14	6379	INFO	Location: Slot: 6 Port: 7 Description: Port Information Reason Code: Enabling Defect Monitoring

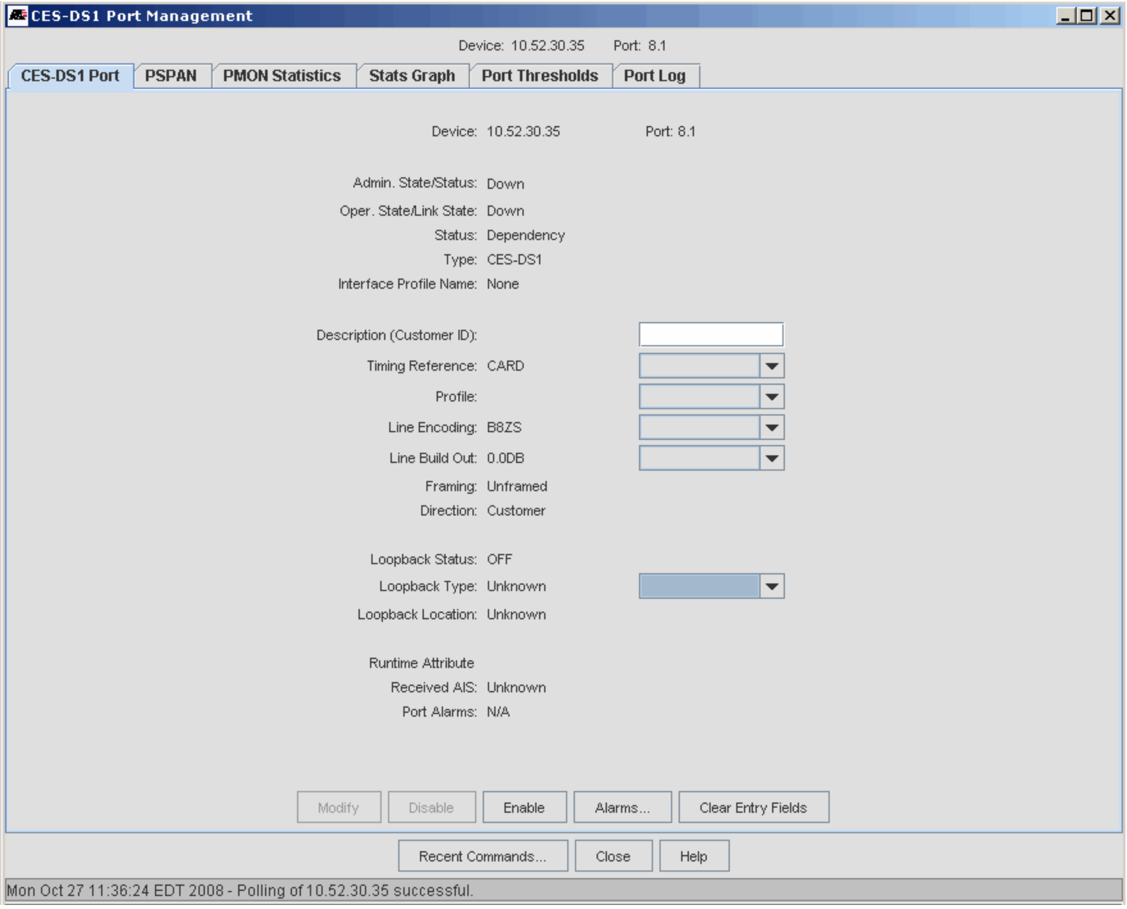
FIGURE 14-50 POTS Port (Port Log Tab)

14.18 CES8 Port (DS1/E1 Port Management Tabbed Form)

The DS1/E1 Port Management Form provides all the relevant information for both single and dual CES endpoints; when the port is part of a dual endpoint configuration, the port dynamically changes so that both endpoints appear in the form.

Note: Refer to "Circuit Emulation Service" on page 623 for a walk-through of provisioning a dual endpoint.

14.18.1 DS1/E1 Port Tab



Device: 10.52.30.35 Port: 8.1

Device: 10.52.30.35 Port: 8.1

Admin. State/Status: Down
Oper. State/Link State: Down
Status: Dependency
Type: CES-DS1
Interface Profile Name: None

Description (Customer ID):
Timing Reference: CARD
Profile:
Line Encoding: B8ZS
Line Build Out: 0.0DB
Framing: Unframed
Direction: Customer

Loopback Status: OFF
Loopback Type: Unknown
Loopback Location: Unknown

Runtime Attribute
Received AIS: Unknown
Port Alarms: N/A

Mon Oct 27 11:36:24 EDT 2008 - Polling of 10.52.30.35 successful.

FIGURE 14-51 CES DS1 Port Tab (For E1, Label and Type are E1)

TABLE 14-20 CES DS1 Port Management - DS1 Port Tab

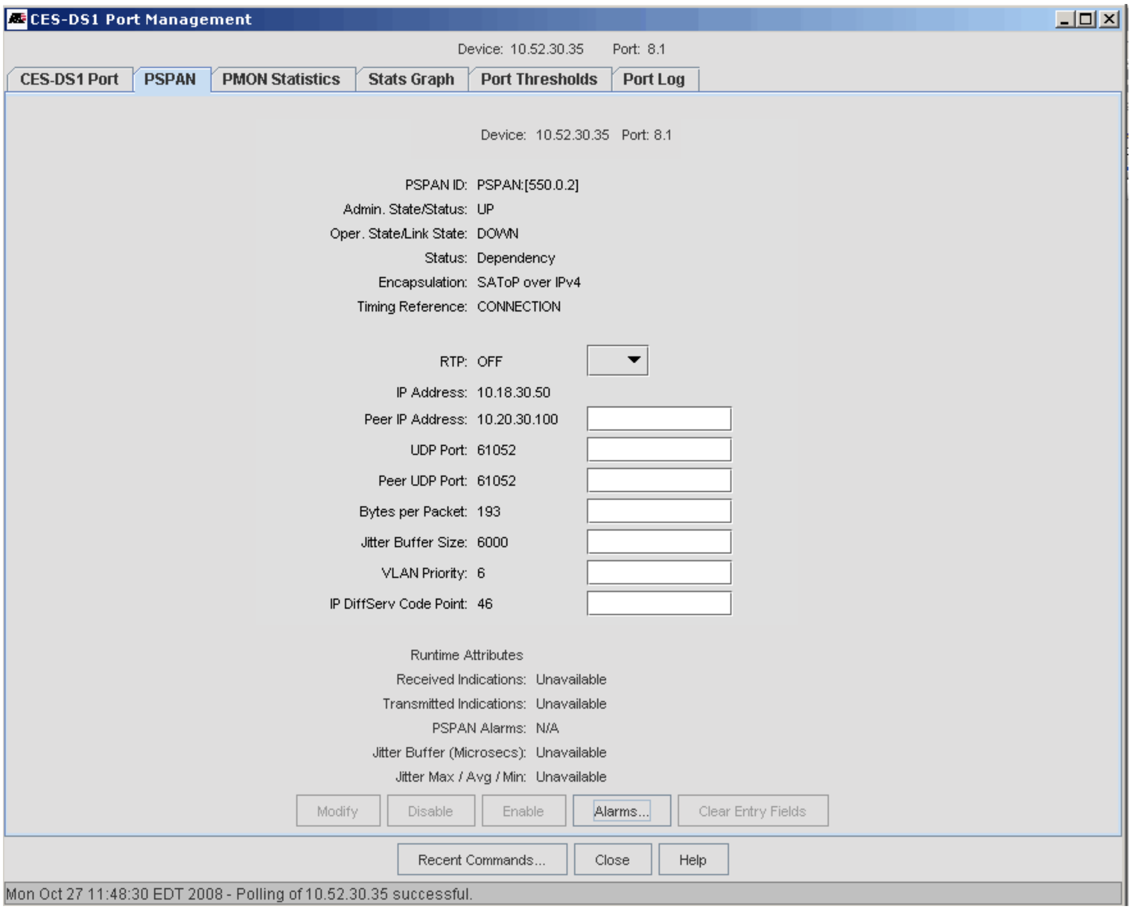
Field/Button	Description
Device: / Port:	Non-editable, this is the port (or ports) that are being displayed.
Admin. State/Status:	Administrative State of the port. This depends on the state of the associated card.
Oper. State/Link Status	Operational State of the port. This depends on the Administrative state of the port.
Status	The same attributes as for other cards
Type:	DS1 or E1
Interface Profile Name:	The port profile being used. This is the first editable field. *Note: A profile must have been previously created.*
Description (Customer ID)	If an active DS1 port, the customer ID that was assigned
Timing Reference	Where the port receives its clocking source from (SELF, CONNECTION, or CARD).
Profile	The profile that was created and applied.
Line Encoding	Either B8ZS or AMI (DS1), or AMI or HDB3 (E1). This should not be changed, unless the card is being re configured.
Line Build Out:	The line build out, either in db (long-haul) or feet (short-haul)

TABLE 14-20 CES DS1 Port Management - DS1 Port Tab

Field/Button	Description
Framing	Always Unframed, since that is the only type of CES currently supported.
Direction	Whether the DS1 interfaces a customer or the network.
Loop Back:	Whether to set the port for loopback, and if so either LINE or INWARD (This is normally done before putting the port in service. The DS1/E1 port is considered operationally DOWN when a loopback is configured, because no “thru service” can be provided. Therefore, when a loopback is configured on the interface, an administratively UP interface would be “UP-DOWN-Loopback”, while an administratively DOWN interface would be DOWN-DOWN-Loopback
Runtime Attribute	What the line is currently processing for alarms
Modify	If any values are changed, this button is enabled.
Disable / Enable	A toggle to enable (if disabled) or disable (if enabled) the port. If the user is disabling the port, there is a warning.
Alarms...	Goes to the Alarm window for the port.
Clear Entry Fields	If any values have been added, they are cleared (including pull-downs).

14.18.2 PSPAN Tab

The PSPAN tab form shows the attributes for the PSPAN that is associated with the port, and, in a dual endpoint configuration, the attributes for the peer PSPAN.



Device: 10.52.30.35 Port: 8.1

Device: 10.52.30.35 Port: 8.1

PSPAN ID: PSPAN:[550.0.2]
Admin. State/Status: UP
Oper. State/Link State: DOWN
Status: Dependency
Encapsulation: SAToP over IPv4
Timing Reference: CONNECTION

RTP: OFF
IP Address: 10.18.30.50
Peer IP Address: 10.20.30.100
UDP Port: 61052
Peer UDP Port: 61052
Bytes per Packet: 193
Jitter Buffer Size: 6000
VLAN Priority: 6
IP DiffServ Code Point: 46

Runtime Attributes
Received Indications: Unavailable
Transmitted Indications: Unavailable
PSPAN Alarms: N/A
Jitter Buffer (Microsecs): Unavailable
Jitter Max / Avg / Min: Unavailable

Mon Oct 27 11:48:30 EDT 2008 - Polling of 10.52.30.35 successful.

FIGURE 14-52 CES PSPAN Tab

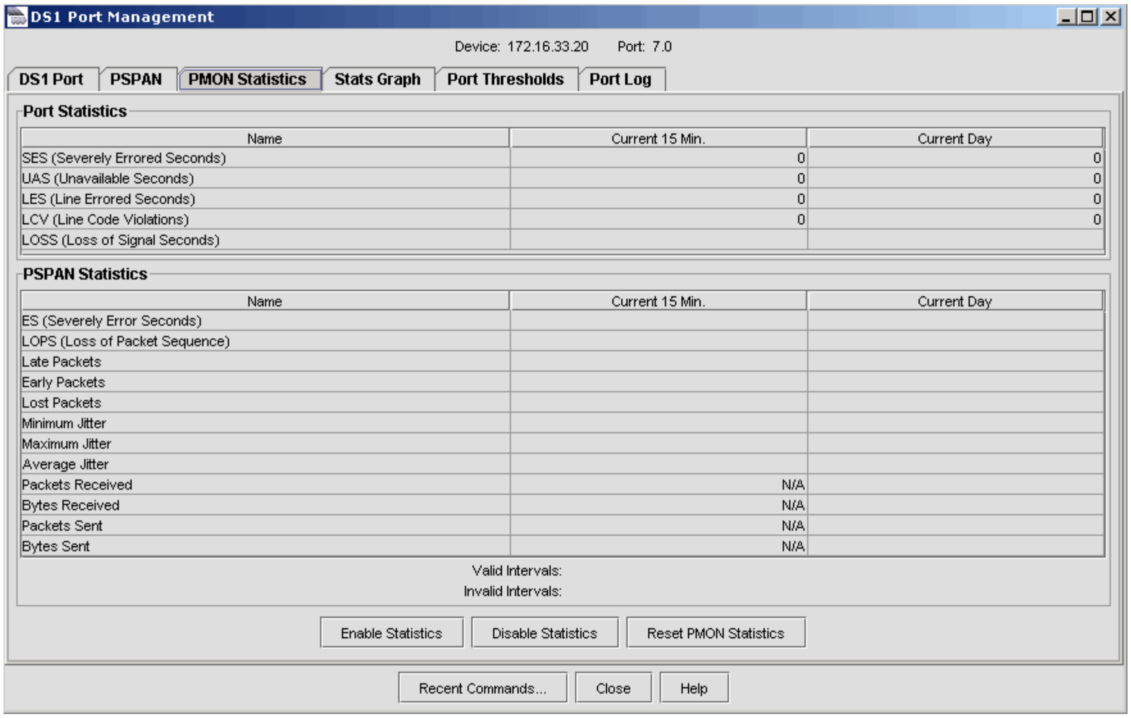
TABLE 14-21 CES DS1 Port Management - PSPAN Tab

Field/Button	Description
PSPAN ID:	This ID is the format vlan:subinterface:pspanid. Note that the subinterface and pspanid are provided by the AlliedView NMS as part of CES provisioning.
Admin. State/Status:	Administrative State of the PSPAN. This depends on the state of the associated port.
Oper. State/Link Status	Operational State of the PSPAN. This depends on the administrative state of the PSPAN.
Status	The status of the PSPAN
Encapsulation:	SAToP over IPv4. This is the only one used for release 5.0
Timing Reference:	Where the PSPAN receives its clocking source from (SELF, CONNECTION, or CARD).
RTP:	Real Time Protocol. RTP must be used if the PSPAN is being used as the timing reference. *Note: This must have the same setting for both sides of a connection.*
IP Address:	IP Address of the connection, In this release, it is for the CES8 card.

TABLE 14-21 CES DS1 Port Management - PSPAN Tab

Field/Button	Description
Peer IP Address:	The IP address for the other end of the connection. \ Note: *By filling in the peer values, the user is explicitly defining the connection; filling in the attributes for the port may define the port but does not actually set up the path through the network.*
UDP Port:	The UDP port for this end of the connection. This must be unique within an IP address on a card
Peer UDP Port:	The UDP at the other end of the connection.
Bytes per Packet:	The default is 193 for DS1, 256 for E1. Note: *Refer to "Circuit Emulation Service" on page 623 on how this is controlled in a dual configuration.*
Jitter Buffer Size:	The size of the jitter buffer.
VLAN Priority	The 802.1p priority bit setting.
IP DiffServ Code Point:	the DSCP (Differentiated Services Code Point) value
RunTime Attributes	The current status of the line.
Modify	If a value has been changed, this button is activated.
Disable / Enable	A toggle to enable (if disabled) or disable (if enabled) the PSPAN. If the user is disabling the PSPAN, there is a warning.
Alarms...	Goes to the Alarms window.
Clear Entry Fields	If any values have been added, they are cleared (including pull-downs).

14.18.3 PMON Statistics



Device: 172.16.33.20 Port: 7.0

Port Statistics

Name	Current 15 Min.	Current Day
SES (Severely Errored Seconds)	0	0
UAS (Unavailable Seconds)	0	0
LES (Line Errored Seconds)	0	0
LCV (Line Code Violations)	0	0
LOSS (Loss of Signal Seconds)		

PSPAN Statistics

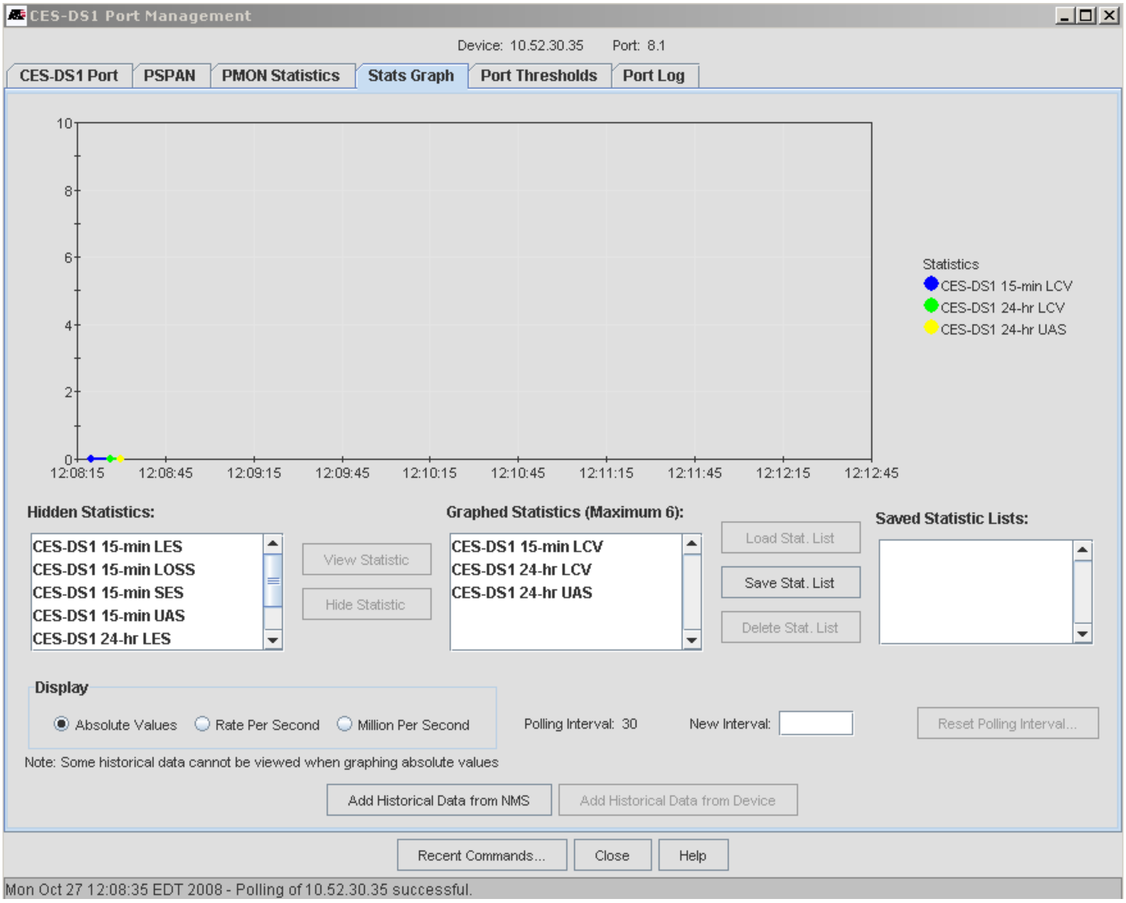
Name	Current 15 Min.	Current Day
ES (Severely Error Seconds)		
LOPS (Loss of Packet Sequence)		
Late Packets		
Early Packets		
Lost Packets		
Minimum Jitter		
Maximum Jitter		
Average Jitter		
Packets Received	N/A	
Bytes Received	N/A	
Packets Sent	N/A	
Bytes Sent	N/A	

Valid Intervals:
Invalid Intervals:

FIGURE 14-53 CES PMON Statistics Tab

- Enable Statistics - Activates all the statistics
- Disable Statistics - Deactivates all the statistics
- Reset Statistics - Sets all the statistics to 0

14.18.4 DS1 Port Management - Stats Graph Tab



Device: 10.52.30.35 Port: 8.1

Hidden Statistics:

CES-DS1 15-min LES
CES-DS1 15-min LOSS
CES-DS1 15-min SES
CES-DS1 15-min UAS
CES-DS1 24-hr LES

Graphed Statistics (Maximum 6):

CES-DS1 15-min LCV
CES-DS1 24-hr LCV
CES-DS1 24-hr UAS

Saved Statistic Lists:

Display

● Absolute Values ○ Rate Per Second ○ Million Per Second

Polling Interval: 30

New Interval:

Note: Some historical data cannot be viewed when graphing absolute values

Mon Oct 27 12:08:35 EDT 2008 - Polling of 10.52.30.35 successful.

FIGURE 14-54 CES DS1 Port Management - Stats Graph Tab

TABLE 14-22 CES DS1 Port Management - Stats Graph Tab

Field/Button	Description
Hidden Statistics:	Statistics not added to the resulting graph
View Statistic:	Enabled when a statistic is chosen form Hidden Statistics, clicking this button adds it to the Graphed Statistics (Maximum of 6), which is the current list of statistics being graphed.
Hide Statistic:	Enabled when a statistic is chosen form Graphed Statistics, clicking this button deletes it from the Graphed Statistics/
Load Stat. List	After choosing one of the names from the Saved Statistic list, the user clicks on this button to make it the current Graphed Statistics
Save Stat. List	The user is prompted to save the current list with a name. Once saved, it is added to the Saved Statistics Lists.

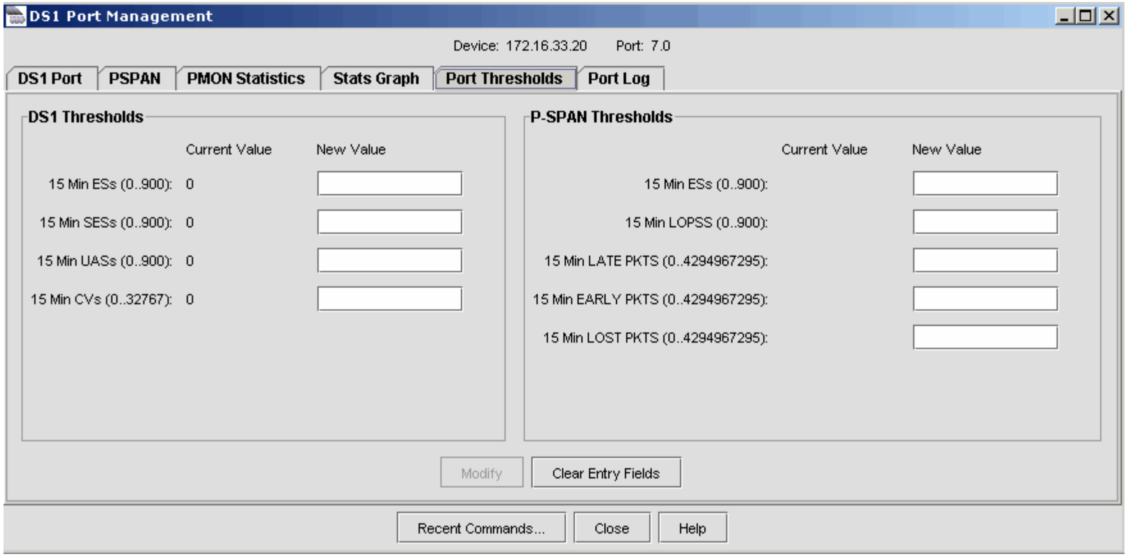
TABLE 14-22 CES DS1 Port Management - Stats Graph Tab

Field/Button	Description
Delete Stat. List	After choosing one of the names from the Saved Statistic list, the user clicks on this button to delete this name.
Display	The attribute that controls the display: - Absolute Values - Rate Per Second - Million Per Second
Polling Interval:	The Current Polling Interval in seconds
New Interval:	Sets a new interval for polling. This is set with the **Reset Polling Interval** button.
Add Historical Data from NMS:	Adds the data collected previously from NMS Performance Management
Add Historical Data from Device:	Adds the data collected previously from the associated device.

14.18.5 DS1 Port Management - Port Thresholds Tab

This form allows the user to modify the threshold values for the DS1/E1 and PSPAN statisitcs.When a new value is entered in the New Value field, the Modify button is enabled.

Note: *In most cases, these DS1/E1 values are not modified because they are part of the DS1/E1 port profile; if the user does change a value, the port is now out of sync with its associated profile, and "* "will appear next to the Profile name on the DS1/E1 Port tab form (as well as the Port Inventory table). In the dual endpoint configuration, the "*" will appear next to the specific port where the values were changed from the Profile. To Resync the port, the user must re-apply the profile on the DS1/E1 tab form, which puts the values back to what they are in the Profile.*



Device: 172.16.33.20 Port: 7.0

DS1 Thresholds

	Current Value	New Value
15 Min ESs (0..900):	0	
15 Min SESs (0..900):	0	
15 Min UASs (0..900):	0	
15 Min CVs (0..32767):	0	

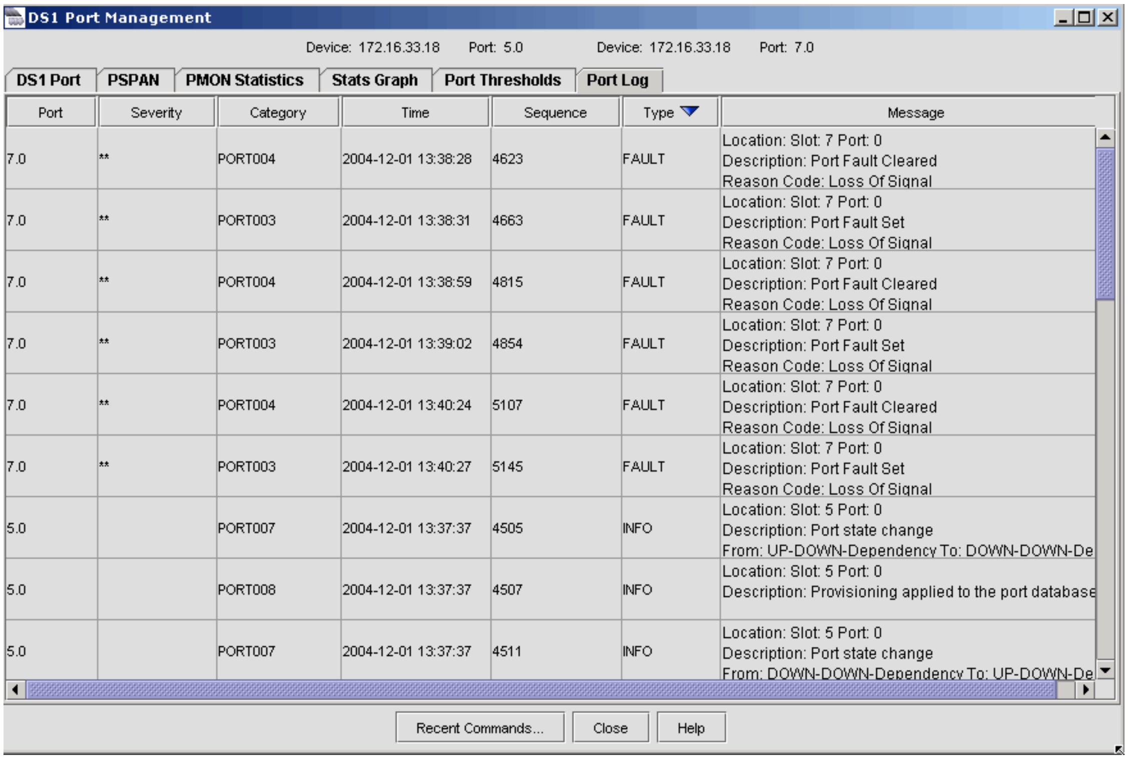
P-SPAN Thresholds

	Current Value	New Value
15 Min ESs (0..900):		
15 Min LOPSS (0..900):		
15 Min LATE PKTS (0..4294967295):		
15 Min EARLY PKTS (0..4294967295):		
15 Min LOST PKTS (0..4294967295):		

FIGURE 14-55 CES DS1 Port Management - Port Thresholds Tab

14.18.6 DS1 Port Management - Port Log Tab

This form lists the PORT logs associated with the port(s) and can therefore provide a history of provisioning as well as any errors or problems. Refer to the following figure.



Device: 172.16.33.18 Port: 5.0 Device: 172.16.33.18 Port: 7.0

Port	Severity	Category	Time	Sequence	Type	Message
7.0	**	PORT004	2004-12-01 13:38:28	4623	FAULT	Location: Slot: 7 Port: 0 Description: Port Fault Cleared Reason Code: Loss Of Signal
7.0	**	PORT003	2004-12-01 13:38:31	4663	FAULT	Location: Slot: 7 Port: 0 Description: Port Fault Set Reason Code: Loss Of Signal
7.0	**	PORT004	2004-12-01 13:38:59	4815	FAULT	Location: Slot: 7 Port: 0 Description: Port Fault Cleared Reason Code: Loss Of Signal
7.0	**	PORT003	2004-12-01 13:39:02	4854	FAULT	Location: Slot: 7 Port: 0 Description: Port Fault Set Reason Code: Loss Of Signal
7.0	**	PORT004	2004-12-01 13:40:24	5107	FAULT	Location: Slot: 7 Port: 0 Description: Port Fault Cleared Reason Code: Loss Of Signal
7.0	**	PORT003	2004-12-01 13:40:27	5145	FAULT	Location: Slot: 7 Port: 0 Description: Port Fault Set Reason Code: Loss Of Signal
5.0		PORT007	2004-12-01 13:37:37	4505	INFO	Location: Slot: 5 Port: 0 Description: Port state change From: UP-DOWN-Dependency To: DOWN-DOWN-De
5.0		PORT008	2004-12-01 13:37:37	4507	INFO	Location: Slot: 5 Port: 0 Description: Provisioning applied to the port database
5.0		PORT007	2004-12-01 13:37:37	4511	INFO	Location: Slot: 5 Port: 0 Description: Port state change From: DOWN-DOWN-Dependency To: UP-DOWN-De

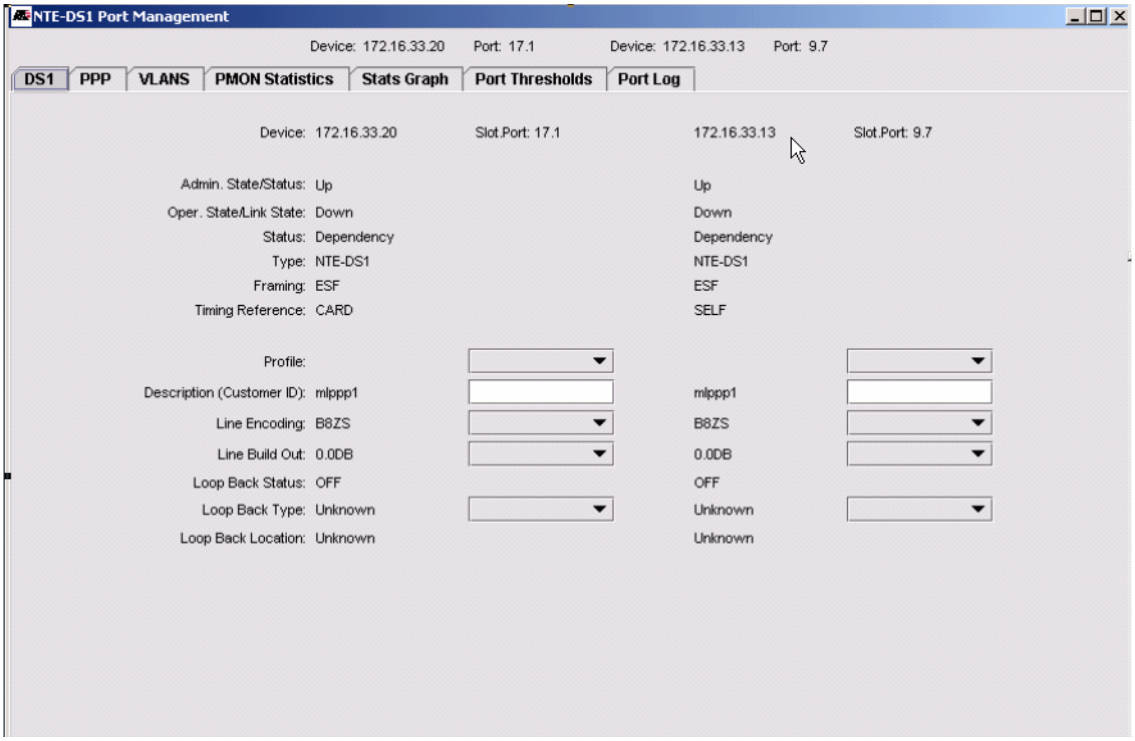
FIGURE 14-56 CES DS1 Port Management - Port Log Tab

14.19 NTE8 Port Management Form

The DS1/E1 Port Management Form for the NTE8 provides all the relevant information for both single and dual NTE8 endpoints; when the port is part of a dual endpoint configuration, the port dynamically changes so that both endpoints appear in the form.

Note: Refer to "NTE8 Dual Circuit Provisioning" on page 653 for a walk-through of provisioning the near and far ends of an NTE8.

14.19.1 DS1/E1 Port Tab



Device: 172.16.33.20 Port: 17.1 Device: 172.16.33.13 Port: 9.7

Device:	172.16.33.20	Slot.Port: 17.1	172.16.33.13	Slot.Port: 9.7
Admin. State/Status:	Up		Up	
Oper. State/Link State:	Down		Down	
Status:	Dependency		Dependency	
Type:	NTE-DS1		NTE-DS1	
Framing:	ESF		ESF	
Timing Reference:	CARD		SELF	
Profile:				
Description (Customer ID):	mlppp1		mlppp1	
Line Encoding:	B8ZS		B8ZS	
Line Build Out:	0.0DB		0.0DB	
Loop Back Status:	OFF		OFF	
Loop Back Type:	Unknown		Unknown	
Loop Back Location:	Unknown		Unknown	

FIGURE 14-57 NTE DS1 Port Management Form - DS1/E1 Tab

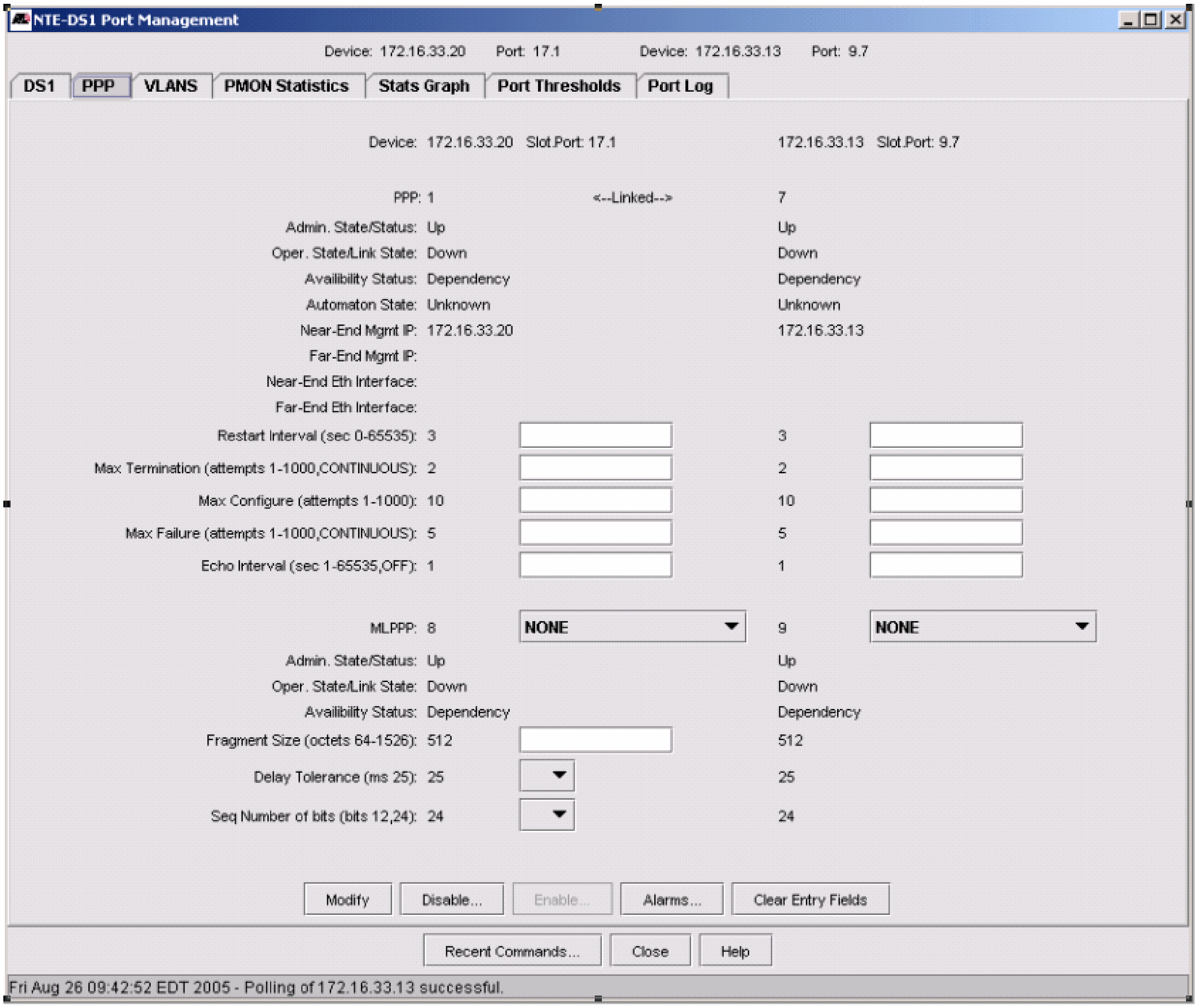
TABLE 14-23 NTE DS1 Port Management - DS1 Port Tab

Field/Button	Description
Device: / Port:	Non-editable, this is the port (or ports) that are being displayed.
Admin. State/Status:	Administrative State of the port. This depends on the state of the associated card.
Oper. State/Link Status	Operational State of the port. This depends on the Administrative state of the port.
Status	The same attributes as for other cards
Type:	NTE-DS1 or NTE-E1
Framing	Always ESF
Timing Reference	Where the port receives its clocking source from (SELF or CARD).
Profile:	The port profile being used. This is the first editable field. *Note: A profile must have been previously created.*
Description	Where the user can add an appropriate description for what the port provides
Line Encoding	Either B8ZS (DS1) or HDB3 (E1). This should not be changed, unless the card is being re configured.
Line Build Out:	The line build out, either in db (long-haul) or feet (short-haul)
Loop Back Status	The DS1/E1 port is considered operationally DOWN when a loopback is configured, because no “thru service” can be provided. Therefore, when a loopback is configured on the interface, an administratively UP interface would be “UP-DOWN-Loopback”", while an administratively DOWN interface would be “DOWN-DOWN-Loopback”

TABLE 14-23 NTE DS1 Port Management - DS1 Port Tab

Field/Button	Description
Loop Back Type	The types of loopback: - NONE - INWARD - Not supported for the NTE8 - LINE - The entire signal is looped from external equipment only through the DS1/E1 port.
Loop Back Location	
Modify	If any values are changed, this button is enabled.
Disable / Enable	A toggle to enable (if disabled) or disable (if enabled) the port. If the user is disabling the port, there is a warning.
Alarms...	Goes to the Alarm window for the port.
Clear Entry Fields	If any values have been added, they are cleared (including pull-downs).

14.19.2 PPP Tab



Device: 172.16.33.20 Port: 17.1 Device: 172.16.33.13 Port: 9.7

Device:	172.16.33.20 Slot.Port: 17.1		172.16.33.13 Slot.Port: 9.7	
PPP:	1	<--Linked-->	7	
Admin. State/Status:	Up		Up	
Oper. State/Link State:	Down		Down	
Availibility Status:	Dependency		Dependency	
Automaton State:	Unknown		Unknown	
Near-End Mgmt IP:	172.16.33.20		172.16.33.13	
Far-End Mgmt IP:				
Near-End Eth Interface:				
Far-End Eth Interface:				
Restart Interval (sec 0-65535):	3		3	
Max Termination (attempts 1-1000,CONTINUOUS):	2		2	
Max Configure (attempts 1-1000):	10		10	
Max Failure (attempts 1-1000,CONTINUOUS):	5		5	
Echo Interval (sec 1-65535,OFF):	1		1	
MLPPP:	8	NONE	9	NONE
Admin. State/Status:	Up		Up	
Oper. State/Link State:	Down		Down	
Availibility Status:	Dependency		Dependency	
Fragment Size (octets 64-1526):	512		512	
Delay Tolerance (ms 25):	25		25	
Seq Number of bits (bits 12,24):	24		24	

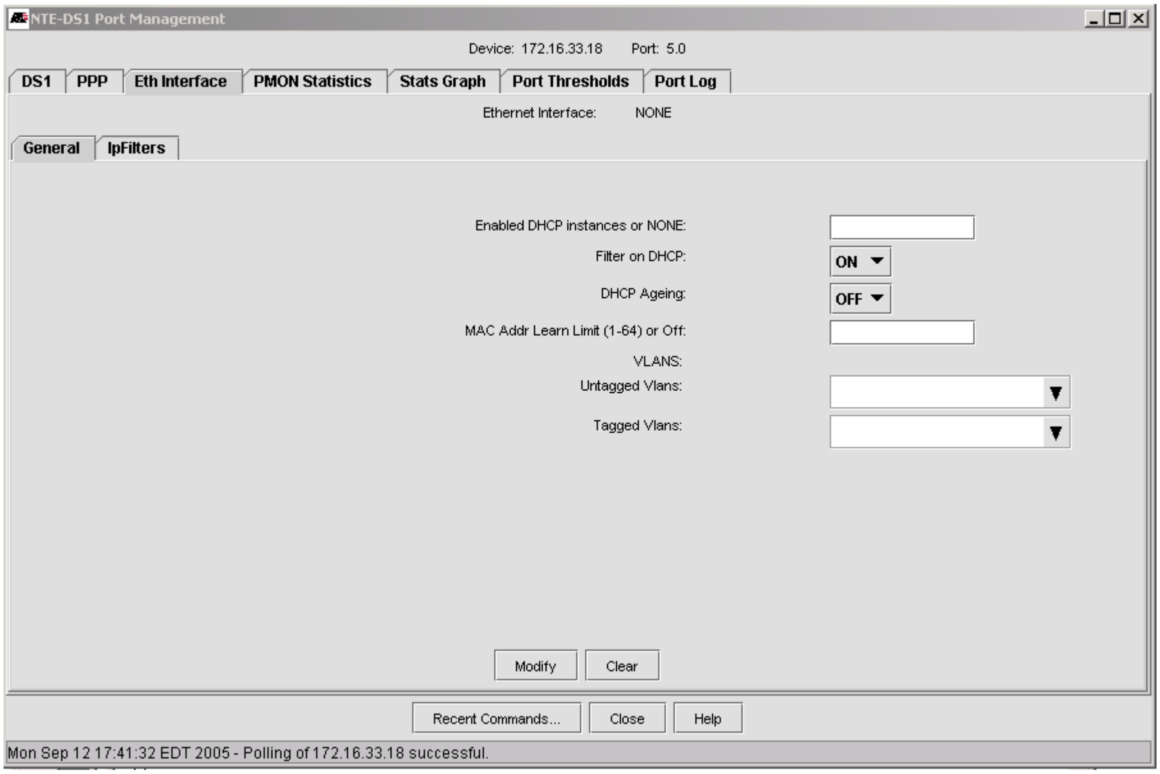
Fri Aug 26 09:42:52 EDT 2005 - Polling of 172.16.33.13 successful.

FIGURE 14-58 NTE DS1 Port Management Form - PPP Tab (Linked Connection)

For information on the parameters, refer to the *Software Reference for iMAP Series Switches*.

14.19.3 Eth Interface Tab

This form has two sub-tabs, General and IpFilters.



Device: 172.16.33.18 Port: 5.0

Ethernet Interface: NONE

Enabled DHCP instances or NONE:

Filter on DHCP: ON

DHCP Ageing: OFF

MAC Addr Learn Limit (1-64) or Off:

VLANS:

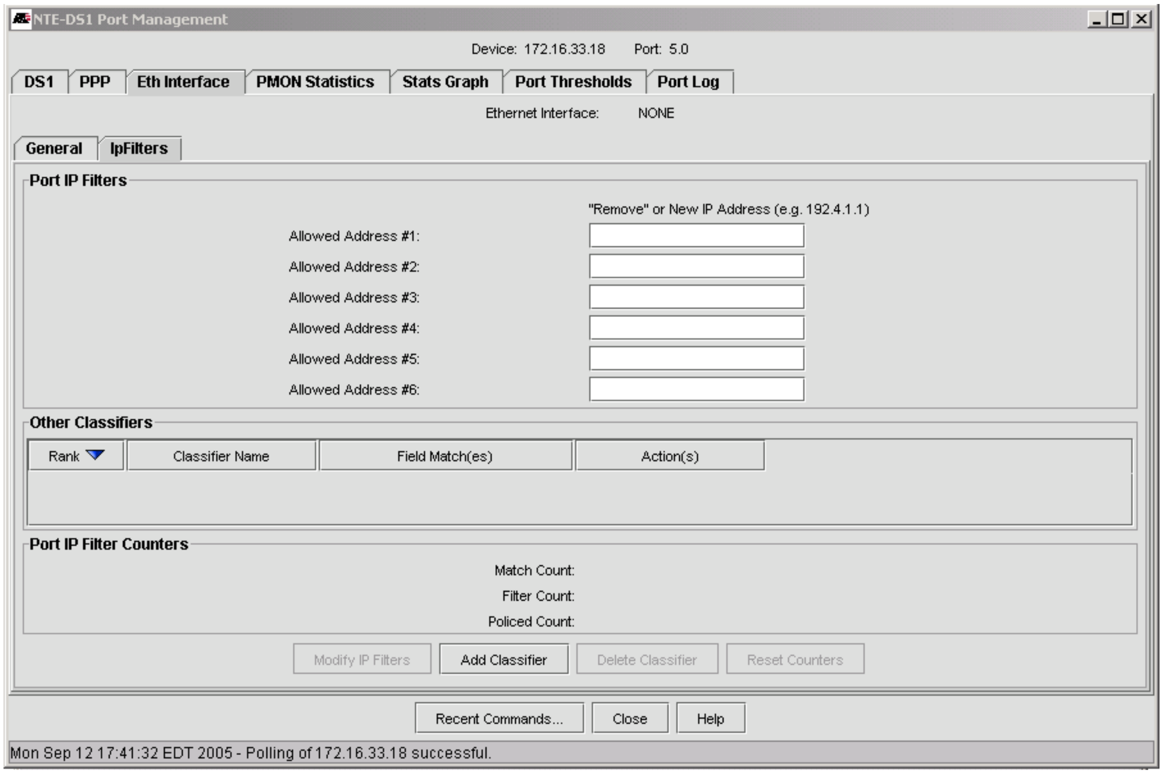
Untagged Vlans:

Tagged Vlans:

Mon Sep 12 17:41:32 EDT 2005 - Polling of 172.16.33.18 successful.

FIGURE 14-59 NTE DS1 Port Management Form - Eth Interface Tab (General)

For information on the parameters, refer to the *Software Reference for iMAP Series Switches*.



Mon Sep 12 17:41:32 EDT 2005 - Polling of 172.16.33.18 successful.

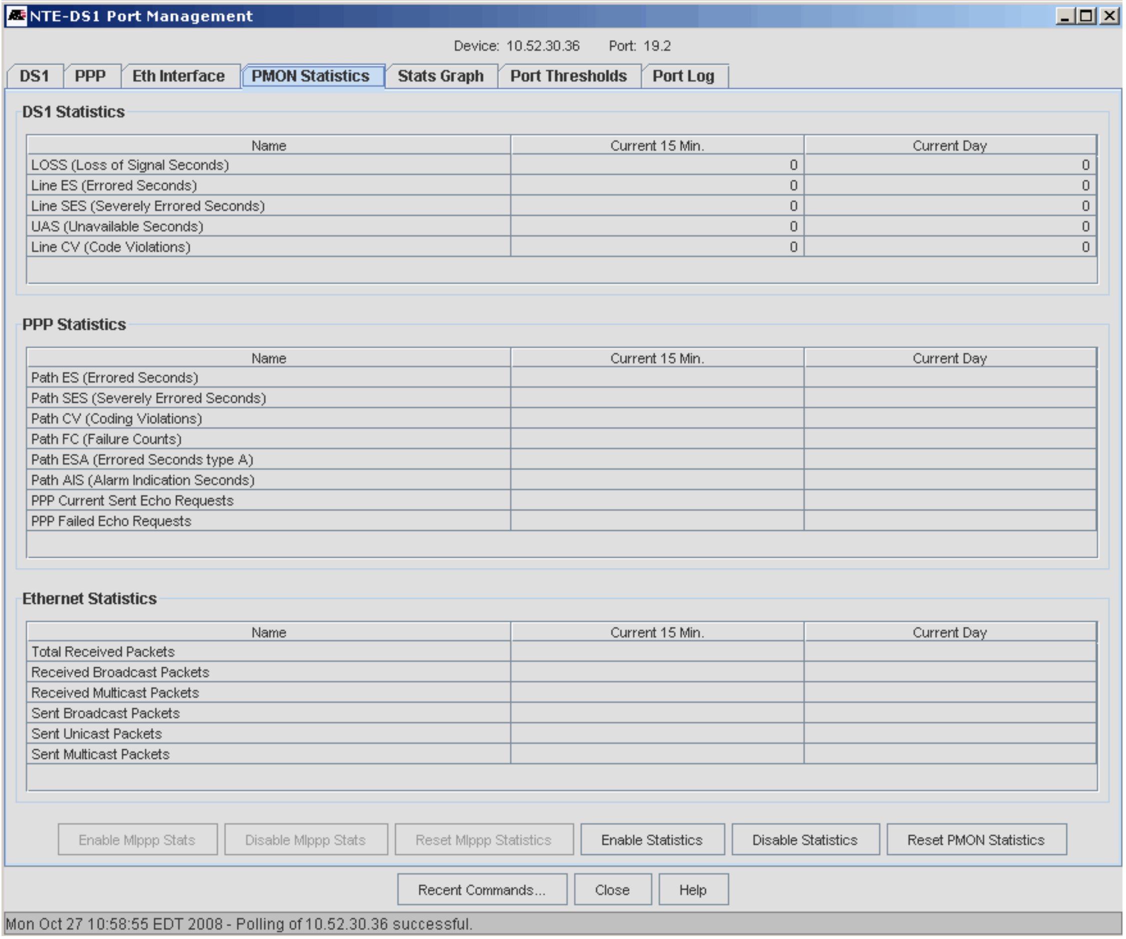
FIGURE 14-60 NTE DS1 Port Management Form - Eth Interface Tab (IpFIlters)

TABLE 14-24 NTE DS1 Port Management - Eth Interface - IP Filters Tab

Field/Button	Description
Allowed Addresses	
Other Classifiers	
Port IP Filter Counters	For the Eth interface the traffic management counters: - Match - Number of packets that match any of the criteria - Filter - Number of packets dropped because they do not match any of the criteria - Policed - Number of non-conforming packets
Add Classifier	Add a Classifier to those that are associated with the interface. The Add Classifier to Port form appears. In this form the user can select a classifier that already exists or create a new classifier with an IP range and Precedence
Delete Classifier	Deletes a classifier chosen from the Classifier (Other Classifiers) list.
Reset Counters	Sets to 0 the Port IP Filter Counters

14.19.4 PMON Statistics Tab

This form allows the user to see the statistics associated with all aspects of the NTE8 port (signal, line, path, and PPP). On a current 15 minutes basis, it includes packet counts.



NTE-DS1 Port Management

Device: 10.52.30.36 Port: 19.2

DS1 Statistics

Name	Current 15 Min.	Current Day
LOSS (Loss of Signal Seconds)	0	0
Line ES (Errored Seconds)	0	0
Line SES (Severely Errored Seconds)	0	0
UAS (Unavailable Seconds)	0	0
Line CV (Code Violations)	0	0

PPP Statistics

Name	Current 15 Min.	Current Day
Path ES (Errored Seconds)		
Path SES (Severely Errored Seconds)		
Path CV (Coding Violations)		
Path FC (Failure Counts)		
Path ESA (Errored Seconds type A)		
Path AIS (Alarm Indication Seconds)		
PPP Current Sent Echo Requests		
PPP Failed Echo Requests		

Ethernet Statistics

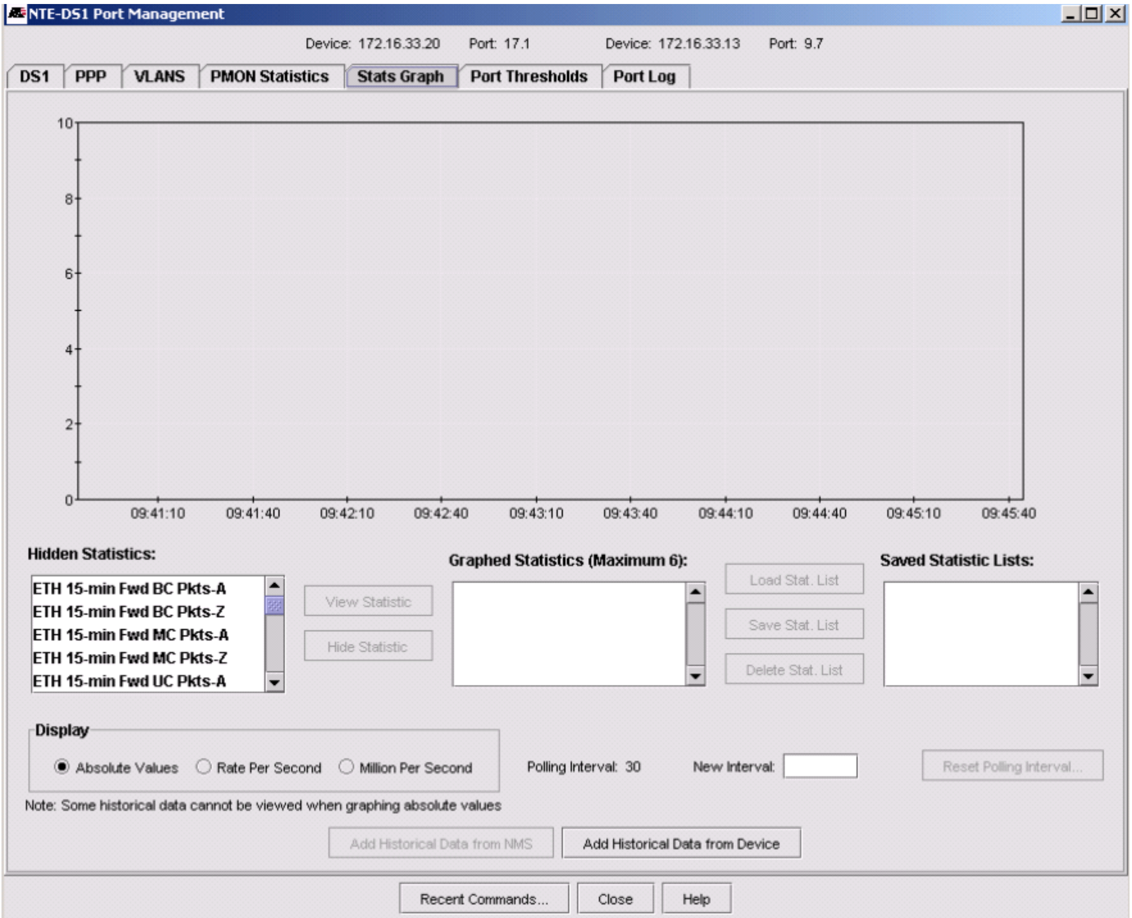
Name	Current 15 Min.	Current Day
Total Received Packets		
Received Broadcast Packets		
Received Multicast Packets		
Sent Broadcast Packets		
Sent Unicast Packets		
Sent Multicast Packets		

Mon Oct 27 10:58:55 EDT 2008 - Polling of 10.52.30.36 successful.

FIGURE 14-61 NTE DS1 Port Management Form - PMON Statistics Tab

- Enable Statistics - Activates all the statistics
- Disable Statistics - Deactivates all the statistics
- Reset Statistics - Sets all the statistics to 0

14.19.5 Stats Graph tab



Device: 172.16.33.20 Port: 17.1 Device: 172.16.33.13 Port: 9.7

Hidden Statistics:

ETH 15-min Fwd BC Pkts-A
ETH 15-min Fwd BC Pkts-Z
ETH 15-min Fwd MC Pkts-A
ETH 15-min Fwd MC Pkts-Z
ETH 15-min Fwd UC Pkts-A

● Absolute Values ○ Rate Per Second ○ Million Per Second

Polling Interval: 30

Note: Some historical data cannot be viewed when graphing absolute values

FIGURE 14-62 NTE DS1 Port Management Form - Stats Graph Tab

TABLE 14-25 NTE DS1 Port Management - Stats Graph Tab

Field/Button	Description
Hidden Statistics:	Statistics not added to the resulting graph
View Statistic:	Enabled when a statistic is chosen form Hidden Statistics, clicking this button adds it to the Graphed Statistics (Maximum of 6), which is the current list of statistics being graphed.
Hide Statistic:	Enabled when a statistic is chosen form Graphed Statistics, clicking this button deletes it from the Graphed Statistics/
Load Stat. List	After choosing one of the names from the Saved Statistic list, the user clicks on this button to make it the current Graphed Statistics
Save Stat. List	The user is prompted to save the current list with a name. Once saved, it is added to the Saved Statistics Lists.
Delete Stat. List	After choosing one of the names from the Saved Statistic list, the user clicks on this button to delete this name.

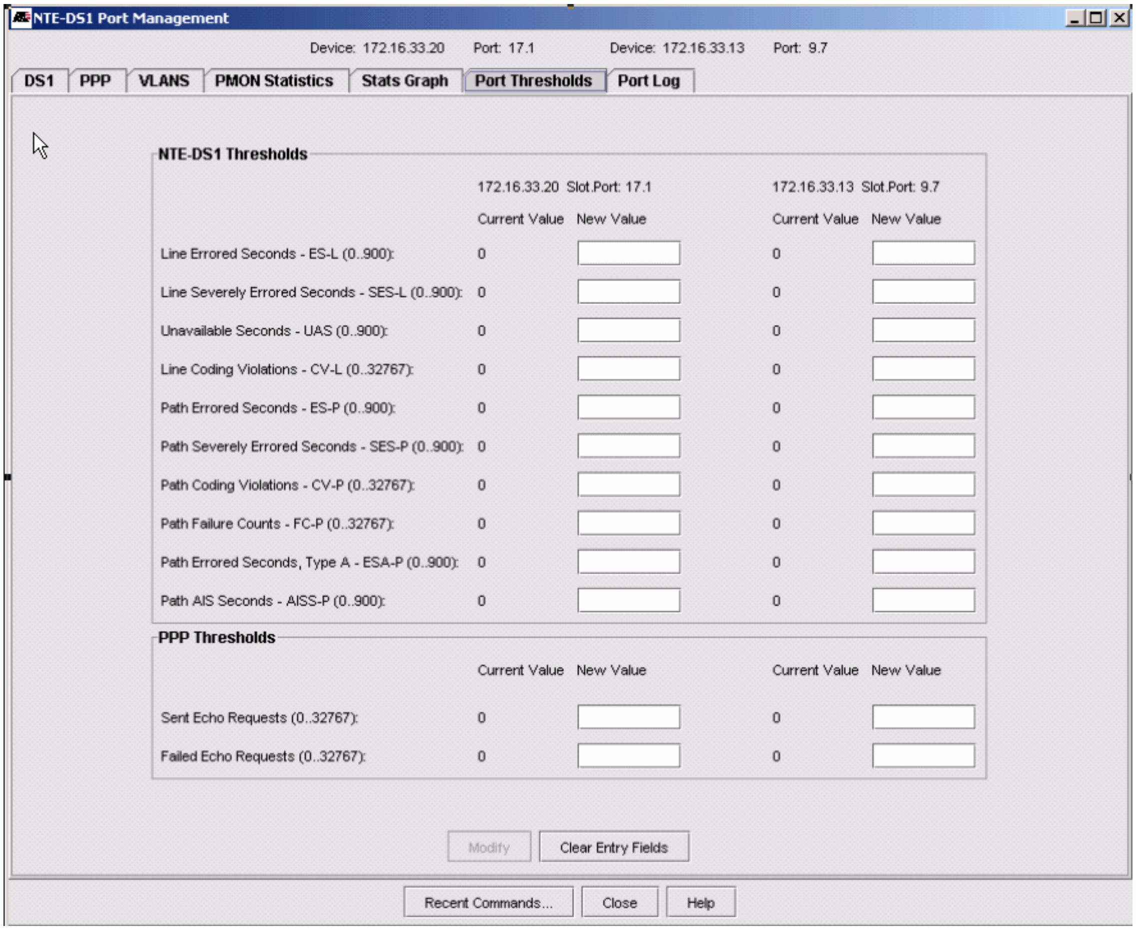
TABLE 14-25 NTE DS1 Port Management - Stats Graph Tab

Field/Button	Description
Display	The attribute that controls the display: - Absolute Values - Rate Per Second - Million Per Second
Polling Interval:	The Current Polling Interval in seconds
New Interval:	Sets a new interval for polling. This is set with the **Reset Polling Interval** button.
Add Historical Data from NMS:	Adds the data collected previously from NMS Performance Management
Add Historical Data from Device:	Adds the data collected previously from the device.

14.19.6 Port Thresholds Tab

This form allows the user to modify the threshold values for the DS1/E1 and PPP statisitcs.When a new value is entered in the New Value field, the Modify button is enabled.

Note: In most cases, these DS1/E1 values are not modified because they are part of the DS1/E1 port profile; if the user does change a value, the port is now out of sync with its associated profile, and " "will appear next to the Profile name on the DS1/E1 Port tab form (as well as the Port Inventory table). In the dual endpoint configuration, the "*" will appear next to the specific port where the values were changed from the Profile. To Resync the port, the user must re-apply the profile on the DS1/E1 tab form, which puts the values back to what they are in the Profile.*



Device: 172.16.33.20 Port: 17.1 Device: 172.16.33.13 Port: 9.7

NTE-DS1 Thresholds

	172.16.33.20 Slot.Port: 17.1		172.16.33.13 Slot.Port: 9.7	
	Current Value	New Value	Current Value	New Value
Line Errored Seconds - ES-L (0..900):	0		0	
Line Severely Errored Seconds - SES-L (0..900):	0		0	
Unavailable Seconds - UAS (0..900):	0		0	
Line Coding Violations - CV-L (0..32767):	0		0	
Path Errored Seconds - ES-P (0..900):	0		0	
Path Severely Errored Seconds - SES-P (0..900):	0		0	
Path Coding Violations - CV-P (0..32767):	0		0	
Path Failure Counts - FC-P (0..32767):	0		0	
Path Errored Seconds, Type A - ESA-P (0..900):	0		0	
Path AIS Seconds - AISS-P (0..900):	0		0	

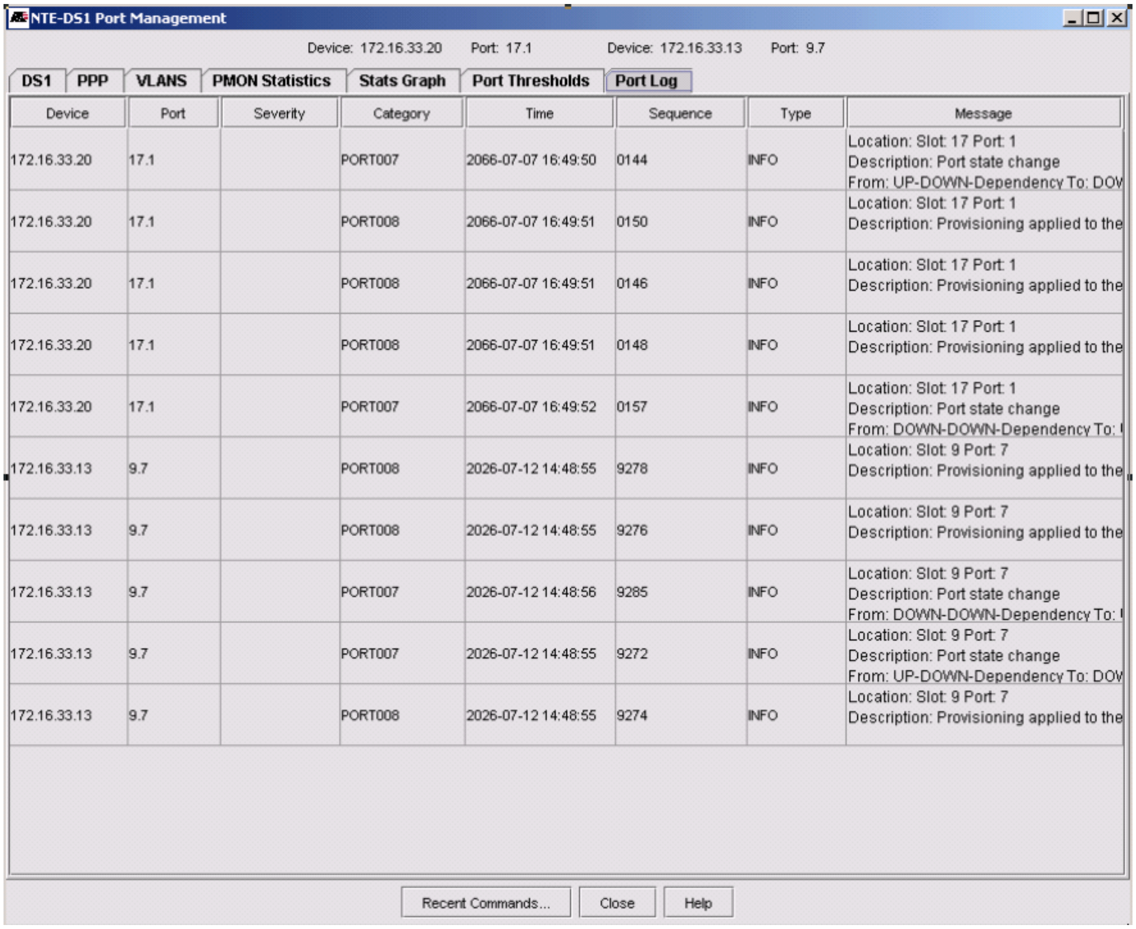
PPP Thresholds

	Current Value	New Value	Current Value	New Value
Sent Echo Requests (0..32767):	0		0	
Failed Echo Requests (0..32767):	0		0	

FIGURE 14-63 NTE DS1 Port Management Form - Stats Graph Tab

14.19.7 DS1 Port Management - Port Log Tab

This form lists the PORT logs associated with the port(s) and can therefore provide a history of provisioning as well as any errors or problems. Refer to the following figure.



Device: 172.16.33.20 Port: 17.1 Device: 172.16.33.13 Port: 9.7

Device	Port	Severity	Category	Time	Sequence	Type	Message
172.16.33.20	17.1		PORT007	2066-07-07 16:49:50	0144	INFO	Location: Slot: 17 Port: 1 Description: Port state change From: UP-DOWN-Dependency To: DOV
172.16.33.20	17.1		PORT008	2066-07-07 16:49:51	0150	INFO	Location: Slot: 17 Port: 1 Description: Provisioning applied to the
172.16.33.20	17.1		PORT008	2066-07-07 16:49:51	0146	INFO	Location: Slot: 17 Port: 1 Description: Provisioning applied to the
172.16.33.20	17.1		PORT008	2066-07-07 16:49:51	0148	INFO	Location: Slot: 17 Port: 1 Description: Provisioning applied to the
172.16.33.20	17.1		PORT007	2066-07-07 16:49:52	0157	INFO	Location: Slot: 17 Port: 1 Description: Port state change From: DOWN-DOWN-Dependency To:
172.16.33.13	9.7		PORT008	2026-07-12 14:48:55	9278	INFO	Location: Slot: 9 Port: 7 Description: Provisioning applied to the
172.16.33.13	9.7		PORT008	2026-07-12 14:48:55	9276	INFO	Location: Slot: 9 Port: 7 Description: Provisioning applied to the
172.16.33.13	9.7		PORT007	2026-07-12 14:48:56	9285	INFO	Location: Slot: 9 Port: 7 Description: Port state change From: DOWN-DOWN-Dependency To:
172.16.33.13	9.7		PORT007	2026-07-12 14:48:55	9272	INFO	Location: Slot: 9 Port: 7 Description: Port state change From: UP-DOWN-Dependency To: DOV
172.16.33.13	9.7		PORT008	2026-07-12 14:48:55	9274	INFO	Location: Slot: 9 Port: 7 Description: Provisioning applied to the

FIGURE 14-64 NTE DS1 Port Management - Port Log Tab

14.20 SHDSL Bonding (Card Level to Port Level)

Originally the SHDLS WireMode was set in the Card Management application. This support will remain for iMAP systems running earlier software version. However, when both of these conditions are true:

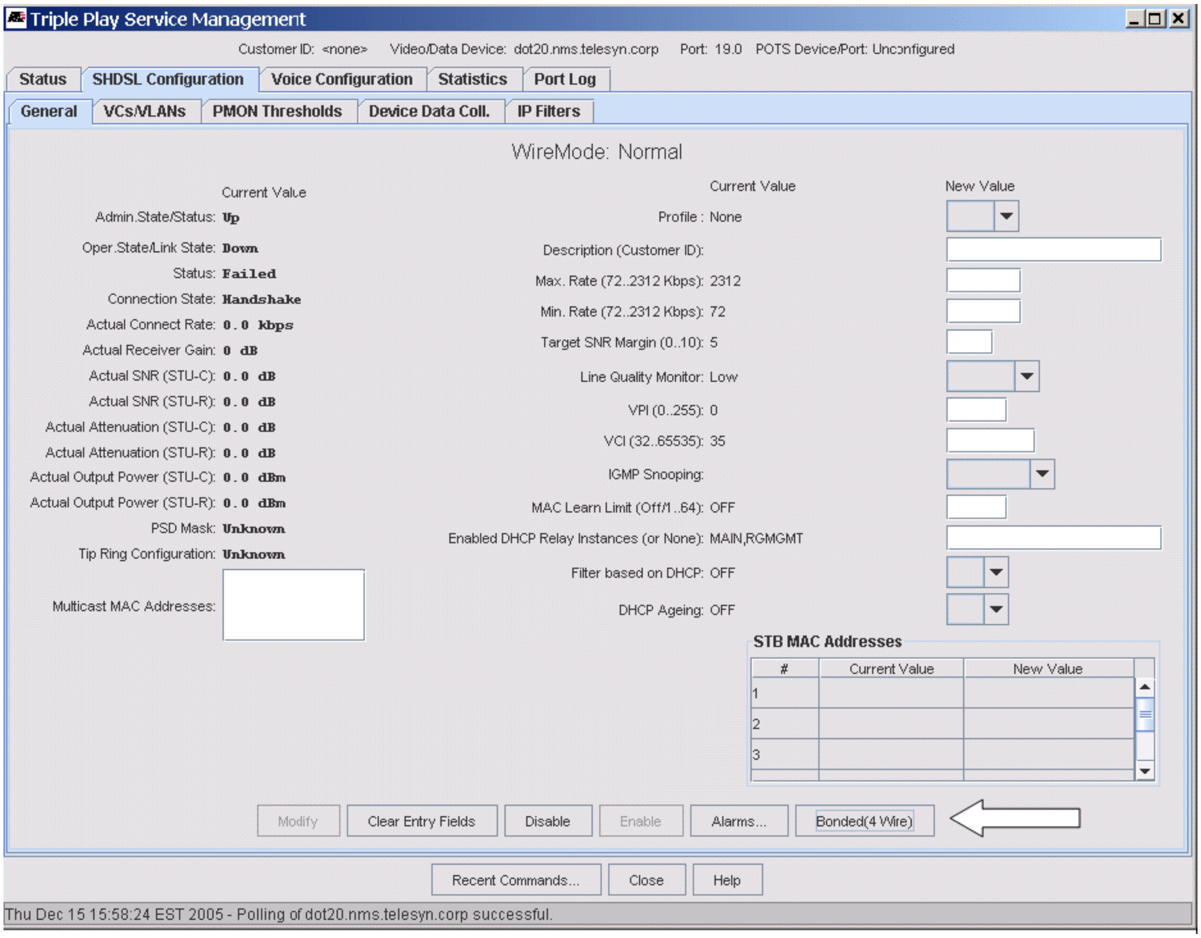
- iMAP systems are running release 7.1 or later, which support port-based bonding
- The AlliedView NMS at release 8.0.

the Port Management application will show the GUI to support bonding.

Impacts on other features are as follows:

- WireMode is **not** added to the SHDSL Port Profile, because it affects the adjacent port, which might already be assigned.
- Both the Port Details window and Triple Play Port Provisioning form will support setting the “WireMode” of **even-numbered** SHDSL ports.

The following figures show these changes.



Customer ID: <none> Video/Data Device: dot20.nms.telesyn.corp Port: 19.0 POTS Device/Port: Unconfigured

WireMode: Normal

Current Value

Admin.State/Status: Up

Oper.State/Link State: Down

Status: Failed

Connection State: Handshake

Actual Connect Rate: 0.0 kbps

Actual Receiver Gain: 0 dB

Actual SNR (STU-C): 0.0 dB

Actual SNR (STU-R): 0.0 dB

Actual Attenuation (STU-C): 0.0 dB

Actual Attenuation (STU-R): 0.0 dB

Actual Output Power (STU-C): 0.0 dBm

Actual Output Power (STU-R): 0.0 dBm

PSD Mask: Unknown

Tip Ring Configuration: Unknown

Multicast MAC Addresses:

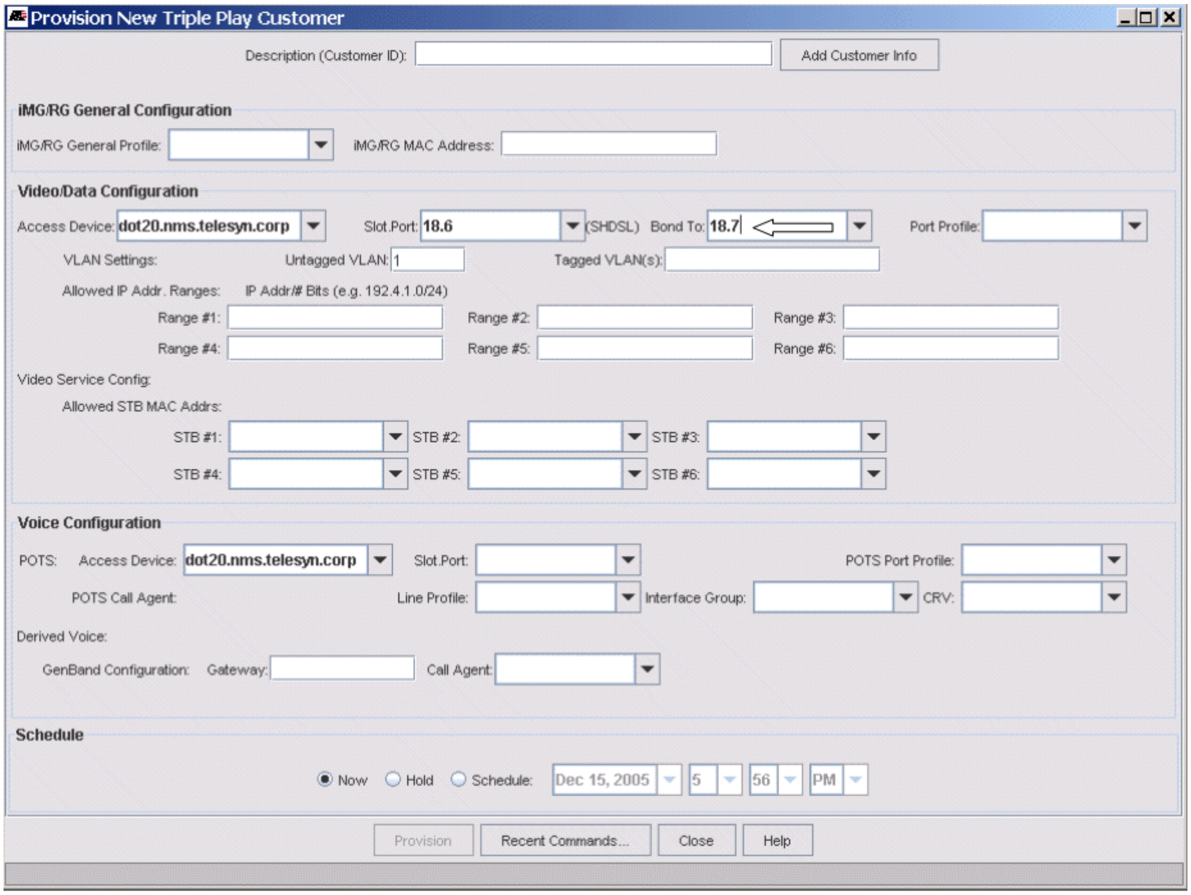
	Current Value	New Value
Profile :	None	
Description (Customer ID):		
Max. Rate (72..2312 Kbps):	2312	
Min. Rate (72..2312 Kbps):	72	
Target SNR Margin (0..10):	5	
Line Quality Monitor:	Low	
VPI (0..255):	0	
VCI (32..65535):	35	
IGMP Snooping:		
MAC Learn Limit (Off/1..64):	OFF	
Enabled DHCP Relay Instances (or None):	MAIN,RGMGMT	
Filter based on DHCP:	OFF	
DHCP Ageing:	OFF	

STB MAC Addresses

#	Current Value	New Value
1		
2		
3		

Thu Dec 15 15:58:24 EST 2005 - Polling of dot20.nms.telesyn.corp successful.

FIGURE 14-65 SHDSL Configuration - General Tab with Bonded Option



Provision New Triple Play Customer

Description (Customer ID):

iMG/RG General Configuration

iMG/RG General Profile: iMG/RG MAC Address:

Video/Data Configuration

Access Device: dot20.nms.telesyn.corp Slot.Port: 18.6 (SHDSL) Bond To: 18.7 Port Profile:

VLAN Settings: Untagged VLAN: 1 Tagged VLAN(s):

Allowed IP Addr. Ranges: IP Addr/# Bits (e.g. 192.4.1.0/24)

Range #1: Range #2: Range #3:

Range #4: Range #5: Range #6:

Video Service Config:

Allowed STB MAC Addrs:

STB #1: STB #2: STB #3:

STB #4: STB #5: STB #6:

Voice Configuration

POTS: Access Device: dot20.nms.telesyn.corp Slot.Port: POTS Port Profile:

POTS Call Agent: Line Profile: Interface Group: CRV:

Derived Voice:

GenBand Configuration: Gateway: Call Agent:

Schedule

● Now ○ Hold ○ Schedule: Dec 15, 2005 5 56 PM

FIGURE 14-66 Triple Play Form for SHDSL with Bonding Option

Using the Triple Play form, individual even numbered ports can be bonded to the next higher odd port. Therefore, when the user selects an even numbered port, the “Bond To:” selector is enabled. Either the next port, or a blank entry, can be selected. Provisioning will set the wire mode appropriately.

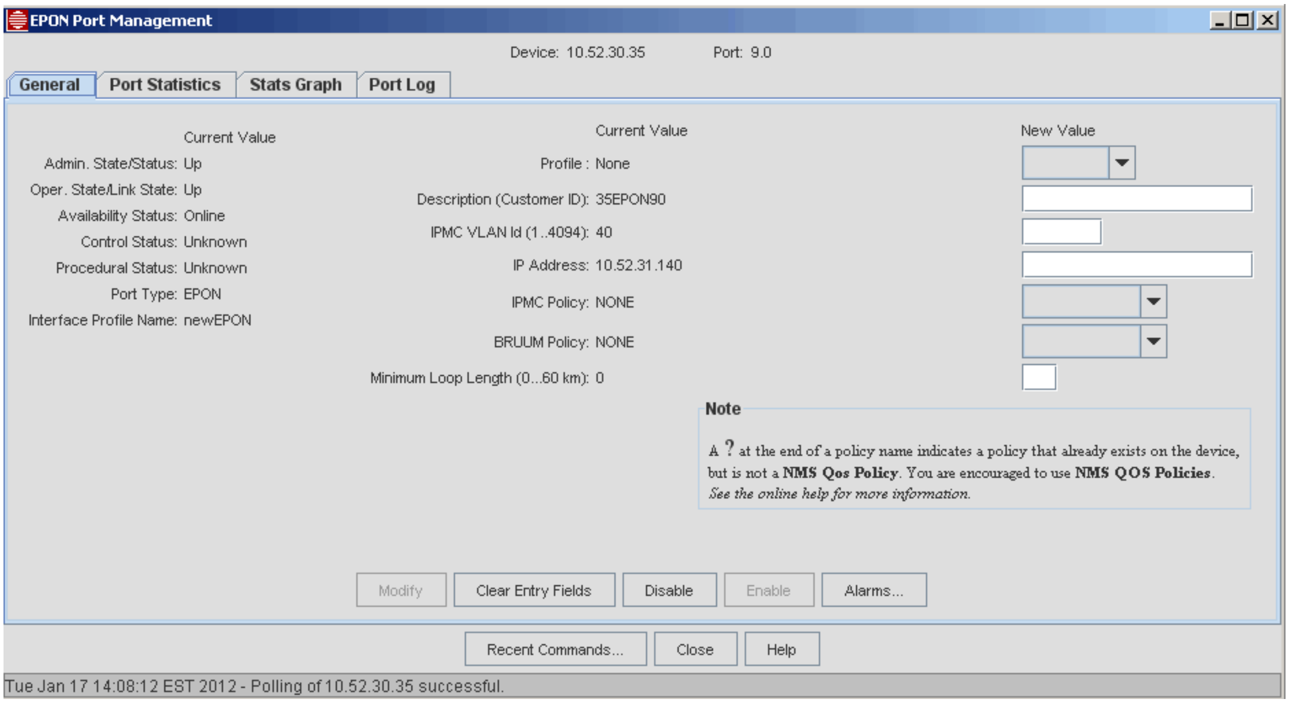
Note: Provisioning will first deprovision a port, which will automatically unbond it, then if necessary it will be rebonded.

As ports are bonded (or unbonded), the following occurs:

- When changing a port on the TriplePlay form, the odd port is removed from the list of ports that can be selected.
- Configuration changes are reflected in the Customer Ports table in Network Inventory.

14.21 View the EPON2 Port Configuration

The EPON2 port corresponds to the OLT on the EPON2 card that connects to up to 32 ONUs. The attributes are shown on the EPON Port Management Form.



Device: 10.52.30.35 Port: 9.0

Current Value

Admin. State/Status: Up
Oper. State/Link State: Up
Availability Status: Online
Control Status: Unknown
Procedural Status: Unknown
Port Type: EPON
Interface Profile Name: newEPON

Current Value / New Value

Profile : None
Description (Customer ID): 35EPON90
IPMC VLAN Id (1..4094): 40
IP Address: 10.52.31.140
IPMC Policy: NONE
BRUUM Policy: NONE
Minimum Loop Length (0...60 km): 0

Note

A ? at the end of a policy name indicates a policy that already exists on the device, but is not a **NMS Qos Policy**. You are encouraged to use **NMS QOS Policies**. *See the online help for more information.*

Tue Jan 17 14:08:12 EST 2012 - Polling of 10.52.30.35 successful.

FIGURE 14-67 EPON Port Management - Tabbed Form

TABLE 14-26 EPON Port Management - General Tab

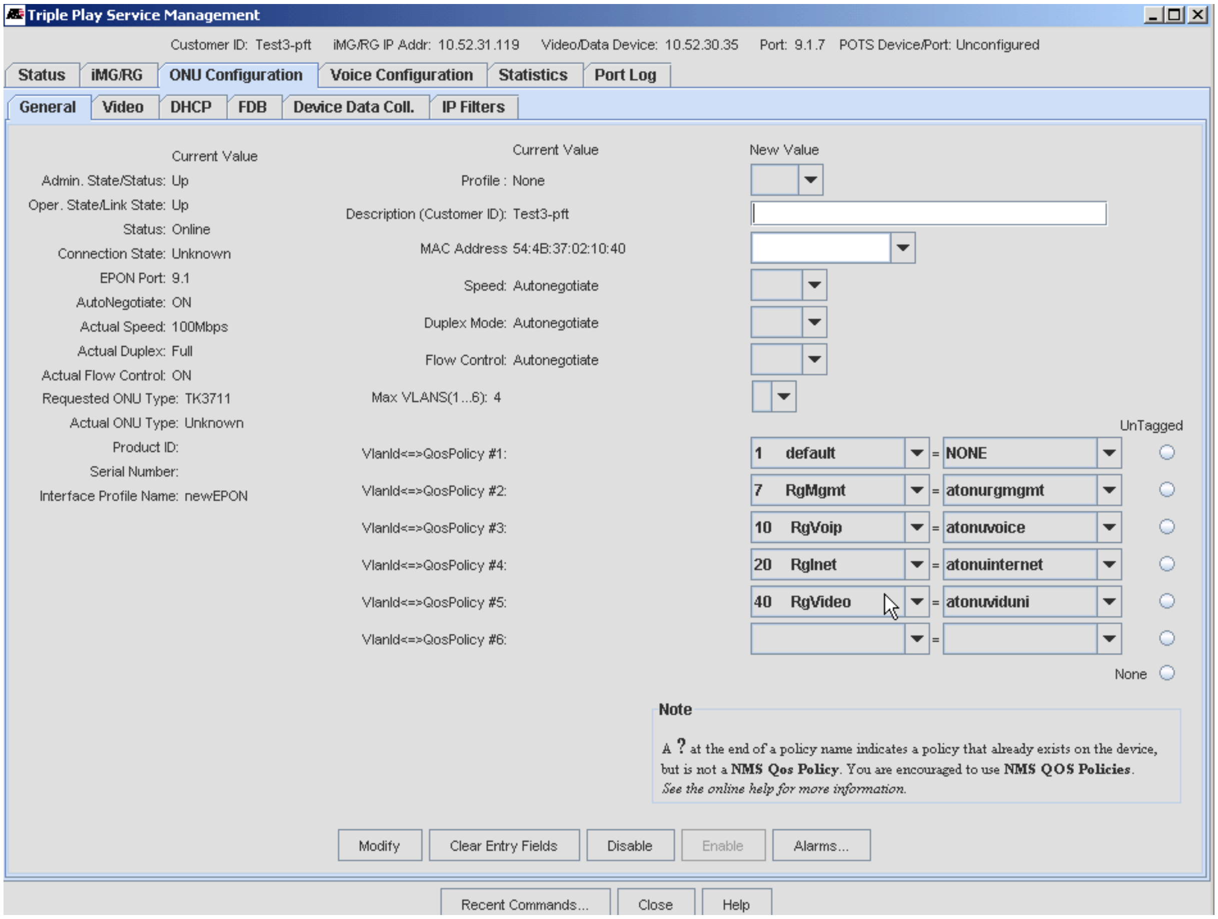
Field/Button	Description
Admin. State/Status	Whether the EPON2 can go into service and therefore pass traffic
Oper. State/Link State	When the Admin State is up, whether the link is passing traffic
Availability Status	Dependency, meaning the state of the upstream component determines this component’s status.
Control Status	
Procedural Status	
Port Type	Always EPON
Profile	The user can create a profile for the EPON2 port and apply it to this port.
Description (Customer ID)	Unique way to identify the port
IPMC VLAN Id (1..4094)	The VLAN that carries downstream multicast traffic
IP Address	Set this to an address that is appropriate for the IPMC subnet. The default 0.0.0.0 may not work as some STBs (such as Amino) require the IPMC IP Address to be set on the EPON interface.
IPMC Policy	The SLA Policy that control the downstream attributes for the IP Multicast VID. (Any upstream attributes are ignored.) This SLA therefore applies to all the ONUs on the EPON2 interface.

TABLE 14-26 EPON Port Management - General Tab

Field/Button	Description
BRUUM Policy	This policy is for the same VID as the downstream-only video stream, but it applies to all upstream traffic from that ONU, and known/learned unicast downstream traffic to that ONU. The ONU/VLAN association and corresponding SLA must be provisioned if unicast or broadcast traffic is required for operation (e.g. DHCP is used for IP address assignment).
Minimum Loop Length (0..60 km)	Allow for setting the allowed distances. The value entered is added to the minimum value of 20, so the maximum is 80 (60 +20). Note that the OLT must be disabled to change this value.

14.22 ONU Configuration (as ON1000 or as part of iMG646PX-ON)

Once the ONU (customer port) is provisioned, the administrator can view the Triple Play Service Management Form and see all of the attributes for the ONU. Note that the Form in this case includes the ONU Configuration tab, as shown in the following figure.



Customer ID: Test3-pft iMG/RG IP Addr: 10.52.31.119 Video/Data Device: 10.52.30.35 Port: 9.1.7 POTS Device/Port: Unconfigured

	Current Value
Admin. State/Status:	Up
Oper. State/Link State:	Up
Status:	Online
Connection State:	Unknown
EPON Port:	9.1
AutoNegotiate:	ON
Actual Speed:	100Mbps
Actual Duplex:	Full
Actual Flow Control:	ON
Requested ONU Type:	TK3711
Actual ONU Type:	Unknown
Product ID:	
Serial Number:	
Interface Profile Name:	newEPON

	Current Value	New Value		UnTagged
Profile :	None			
Description (Customer ID):	Test3-pft			
MAC Address	54:4B:37:02:10:40			
Speed:	Autonegotiate			
Duplex Mode:	Autonegotiate			
Flow Control:	Autonegotiate			
Max VLANS(1...6):	4			
VlanId<=>QosPolicy #1:		1 default	= NONE	○
VlanId<=>QosPolicy #2:		7 RgMgmt	= atonurgmgmt	○
VlanId<=>QosPolicy #3:		10 RgVoip	= atonuvoice	○
VlanId<=>QosPolicy #4:		20 RgInet	= atonuinternet	○
VlanId<=>QosPolicy #5:		40 RgVideo	= atonuviduni	○
VlanId<=>QosPolicy #6:			=	○
			None	○

Note

A ? at the end of a policy name indicates a policy that already exists on the device, but is not a **NMS Qos Policy**. You are encouraged to use **NMS QOS Policies**. *See the online help for more information.*

FIGURE 14-68 Service Management Form for ONU

Because this reflects the ONU configuration, there are attributes that are unique on the lower part of the Form. For the ONU, the user creates on the iMAP QoS policies that are the association of a VLAN and the ONU. These usually reflect the kind of traffic the VLAN will carry. The Form can list the up to six VLANs that can be provisioned. In most cases five are configured for Triple Play, with three for the services, one for the RGMgmt VLAN, and one for a class of traffic called BRUUM.

The user can see the VLAN id and QoS Policy as highlighted in the figure. The default QoS policy is named “NONE” and can be associated with one or more VLANs. The user has the option of selecting **one** of the VLANs as the **untagged** VLAN, and so the selection uses a radio button.

Note: Refer to "Example of an EPON/ONU Interface Policy" on page 253 for details on policies for the EPON/ONU.

Note: Refer to "Provisioning iMGs" on page 763 for complete information on provisioning the iMG/RG.

As with other port type configuration tabs, the Video Tab includes the IGMP / multicast information.

14.23 VDSL24 Port

In the VDSL configuration, a VDSL modem is connected to the VDSL24 card. With the higher bandwidth, services such as HDTV are supported.

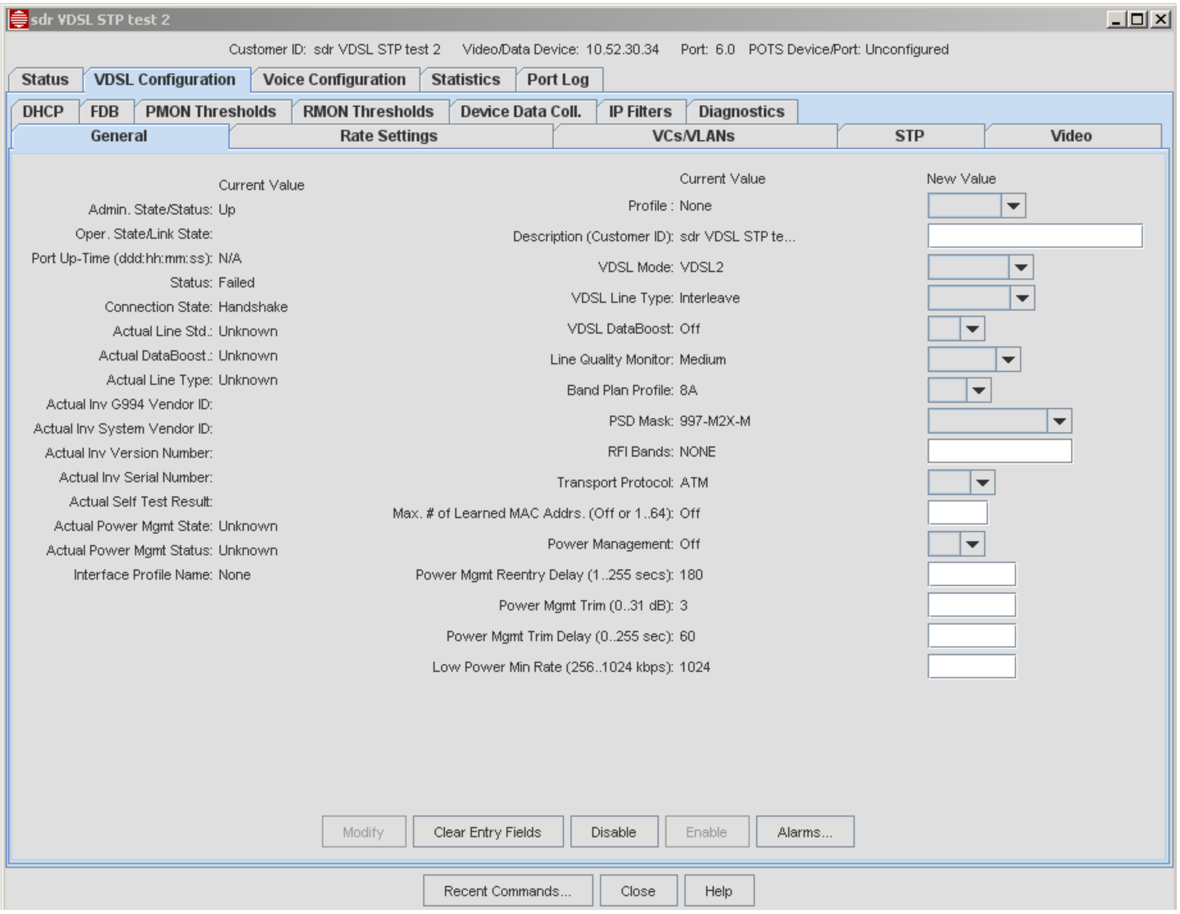
Note that the interface can support ADSL (ADSL2+) as well as VDSL2 mode. To switch modes, the user must disable the interface, and then switch modes on this form.

14.23.1 VDSL Configuration - General Tab

This screen includes all the attributes that define the port, as show in the following figure.

As with the VDSL Port Profile, general parameters on the VDSL View/Modify screen are redistributed from one to two tabs. Power management parameters are added to the updated General tab and the other rate-related parameters are moved to the Rate Settings tab. As with ADSL, the read-only parameters are added to the left and the modifiable parameters are added to the right.

Although power management parameters will be left off the screen when the iMAP release is less than 11.0.0, the remaining general parameters will still be distributed between the General and Rate Settings tabs



Customer ID: sdr VDSL STP test 2 Video/Data Device: 10.52.30.34 Port: 6.0 POTS Device/Port: Unconfigured

	Current Value
Admin. State/Status:	Up
Oper. State/Link State:	
Port Up-Time (ddd:hh:mm:ss):	N/A
Status:	Failed
Connection State:	Handshake
Actual Line Std.:	Unknown
Actual DataBoost.:	Unknown
Actual Line Type:	Unknown
Actual Inv G994 Vendor ID:	
Actual Inv System Vendor ID:	
Actual Inv Version Number:	
Actual Inv Serial Number:	
Actual Self Test Result:	
Actual Power Mgmt State:	Unknown
Actual Power Mgmt Status:	Unknown
Interface Profile Name:	None

	Current Value	New Value
Profile :	None	
Description (Customer ID):	sdr VDSL STP te...	
VDSL Mode:	VDSL2	
VDSL Line Type:	Interleave	
VDSL DataBoost:	Off	
Line Quality Monitor:	Medium	
Band Plan Profile:	8A	
PSD Mask:	997-M2X-M	
RFI Bands:	NONE	
Transport Protocol:	ATM	
Max. # of Learned MAC Addrs. (Off or 1..64):	Off	
Power Management:	Off	
Power Mgmt Reentry Delay (1..255 secs):	180	
Power Mgmt Trim (0..31 dB):	3	
Power Mgmt Trim Delay (0..255 sec):	60	
Low Power Min Rate (256..1024 kbps):	1024	

FIGURE 14-69 VDSL Configuration - General Tab

TABLE 14-27 VDSL Configuration Form, General Tab

Field/Button	Description
Admin. State/Status	The Administrative State can be controlled and determines the Operational State.
Oper. State/Link State	The ability of the port to provide service. The Administrative State must be up and then the system determines if the port can provide service.
Port Up-Time	Amount of time the physical interface has been in the UP-UP-Online state.
Status	The status of the port that follows form the Administrative State and Operational State. For meanings, refer to the *Software Reference for iMAP Series Switches*. - ONLINE - IN TEST - FAILED - OFFLINE - DEPENDENCY - DEGRADED - NOT INSTALLED - INITIALIZATION REQUIRED - TERMINATING

TABLE 14-27 VDSL Configuration Form, General Tab (Continued)

Field/Button	Description
Connection State	The connection state, such as Idle or Showtime
Actual Line Std.	The line standard that was actually chosen.
Actual Databoost	Whether the DATABOOST feature has been implemented
Actual Line Type	The line type that was actually chosen.
Actual Inv G994 Vendor ID	To Be Supplied
Actual Inv System Vendor ID	To Be Supplied
Actual Inv Version Number	To Be Supplied
Actual Inv Serial Number	To Be Supplied
Actual Self Test Result	To Be Supplied
Actual Power Mgmt State	The state the interface is in for power reduction (Full On, Low Power, Idle)
Actual Power Mgmt Status	Whether the power management feature has been activated for the interface
Interface Profile Name	Which profile is being used (AutoProv or none, which uses default values).
Profile	Enter another VDSL Profile Name
Description (Customer ID)	An ID that can be given to uniquely identify the port. In most cases, the subscriber’s telephone number is used. Refer to "Naming Convention for Customer IDs (Triple Play Form)" on page 780.
VDSL Mode	Specifies the mode for the VDSL port. For the VDSL24A and VDSL24B cards, VDSL2 is the default. The parameters that are provisionable depend on whether the VDSL2 or ADSL mode is chosen
VDSL Line Type	Defines the type of VDSL physical line entity that exists, by defining whether and how the line is channelized.
VDSL Databoost	Whether the Databoost feature has been provisioned
Line Quality Monitor	The level the line quality monitor has been set at. Refer to the *Software Reference for iMAP Series Switches*.
Band Plan Profile	Band plan profile for frequency settings. The band plan determines the transmission frequencies used when transmitting and receiving data between the interface and the modem
PSD Limit Mask	VDSL/ADSL power spectrum density limits are defined by the band plan. The various standard bodies have defined a number of band plans that have regional significance. The masks define shaping parameters for the signal, including Annex A or Annex B
RFI Bands	Specifies the radio frequency interference bands to filter from the VDSL link. To avoid interference it is necessary to introduce power control (notching) in one or more of these bands.
Transport Protocol	Used to specify the type of transport used when operating in VDSL mode. When running in ATM mode, the VDSL interface can automatically toggle to ADSL if the modem at the other end of the connection is ADSL. PTM (Packet Transport Mode) requires both ends of the connection to be VDSL compliant If the Transport Protocol is changed from ATM to PTM, there is a warning that VCs are not supported, and any existing VCs will be removed from the port.
Max. # of Learned MAC Addrs.	Depending on feature provisioning, the number of MAC addresses that can be learned (or Off)
Power Management	Changes the current power management state.

TABLE 14-27 VDSL Configuration Form, General Tab (Continued)

Field/Button	Description
Power Mgmt Reentry Delay	The amount of time that must elapse before re-entering the Low Power state after a transition to the Full On state. (Should not be set to a value less than 120 seconds)
Power Mgmt Trim	The maximum aggregate transmit power reduction (trimming) that can be performed with each power trim operation in the Low Power state.
Power Mgmt Trim Delay	The amount of time that must elapse before an additional reduction (trimming) of power occurs in the Low Power state.
Low Power Min Rate	The minimum net data rate for the bearer channel while operating in the Low Power state. The value for LOWPOWERRATE must be between MAXDOWNSTREAMRATE and MINDOWNSTREAMRATE
Modify	Enabled when a value in New Value field has been entered, modifies the attributes according to the updated values.There is an error message if a value is invalid.
Clear Entry Fields	Clear any fields that have been datafilled but not yet Modified
Enable	Enabled if the port is in an Administrative State of DOWN, enables the port and so brings the Administrative State to UP. If possible (for example, the VDSL2 card must be enabled), the Operational State will change to UP.
Disable	Enabled if the port is in an Administrative State of UP, disables the port and so brings the Administrative State to DOWN. The Operational State will also change to DOWN.
Alarms	Invokes the Alarm table of the Fault Management Object.

TABLE 14-28 VDSL Configuration Form, Rate Settings Tab

Field/Button	Description
Actual Connect Rate	The upstream/downstream rate that was actually attained.
Max. Attainable Rate	The possible upstream/downstream rate according to dsl type and mode.
Actual SNR (Near End/Far End)	The signal-noise ratio for near end/far end that was actually attained.
Actual Attenuation (Near End/Far End)	The attenutation for near end/far end that was actually attained.
Actual Output Power (Near End/Far End)	The output power achieved for near end/far end.
Actual Upstream/ Downstream PSD	The actual transmit upstream PSD setting.
Actual Upstream/ Downstream INP	The actual impulse noise protection value for upstream
Max. Upstream Rate	Specifies the maximum upstream bit rate to attain for a VDSL port. The valid range for this parameter is from 32Kb to 14848. Leaving this rate to the default of 10000 (10Mbps) ensures the higher downstream rates (50 Mbps) for VDSL
Min. Upstream Rate	Specifies the minimum upstream bit rate to attain for a VDSL port. The MINUPSTREAMRATE must be equal or less than the MAXUPSTREAMRATE
Max. Downstream Rate	Specifies the maximum downstream bit rate to attain for a VDSL port. The valid range for this parameter for VDSL is from 32Kb to51200Kb
Min. Downstream Rate	Specifies the minimum downstream bit rate to attain for a VDSL port. The valid range for VDSL is from 32Kb to51200Kb. The MINDOWNSTREAMRATE must be less than the MAXDOWNSTREAMRATE.

TABLE 14-28 VDSL Configuration Form, Rate Settings Tab (Continued)

Field/Button	Description
Max. Downstream Interleave Delay	Specifies the maximum interleave delay in milliseconds used when the VDSL linetype is set to INTERLEAVE.
Max. Upstream Interleave Delay	Specifies the maximum interleave delay in milliseconds used when the VDSL linetype is set to INTERLEAVE.
Target SNR Ratio Margin	Specifies the target signal-to-noise ratio (in dB) to achieve on a VDSL port. The valid range is 0 to 30 for a VDSL interface, with the default 0 for a VDSL interface. This allows the operator to adjust the signal characteristics to account for such things as known noise in the binder group, extreme length of a loop, or other issues in the copper plant
Max. SNR Margin	Used to set the maximum signal-to-noise ratio supported by the interface. The value for this parameter must be greater than the value for Target SNR Margin. Optionally, this parameter can be set to 'OFF' which eliminates any maximum limit for SNR.
Min. SNR Margin	Sets the minimum signal-to-noise ratio supported by the interface. The value for this parameter must be less than the value for Target SNR Margin. Optionally, this parameter can be set to OFF which eliminates any minimum limit for SNR.
Max. Upstream Nominal PSD	VDSL/ADSL power spectrum density limits are defined by the band plan and determine this value.
Max. Downstream Nominal PSD	VDSL/ADSL power spectrum density limits are defined by the band plan and determine this value.
Max. Receive Power	Specifies the maximum received power level in dBm received from the modem before the interface is alarmed and disabled.
Minimum Upstream INP	Sets the minimum impulse noise protection value for upstream.
Minimum Downstream INP	Sets the minimum impulse noise protection value for downstream.
Modify	Enabled when a value in New Value field has been entered, modifies the attributes according to the updated values.There is an error message if a value is invalid.
Clear Entry Fields	Clear any fields that have been datafilled but not yet Modified
Enable	Enabled if the port is in an Administrative State of DOWN, enables the port and so brings the Administrative State to UP. If possible (for example, the VDSL2 card must be enabled), the Operational State will change to UP.
Disable	Enabled if the port is in an Administrative State of UP, disables the port and so brings the Administrative State to DOWN. The Operational State will also change to DOWN.
Alarms	Invokes the Alarm table of the Fault Management Object.

14.23.2 VDSL Configuration - VCs/VLANs Tab

This screen is determined by the mode of the port. If the port is in VDSL mode and using ATM, there is only a VPI/VCI of 0/35 that cannot be changed. If the port is in VDSL mode and using PTM, there is no VCI, only a data channel. In ADSL mode, the VPI/VCI follow the ADSL configuration (up to four VPI/VCI).

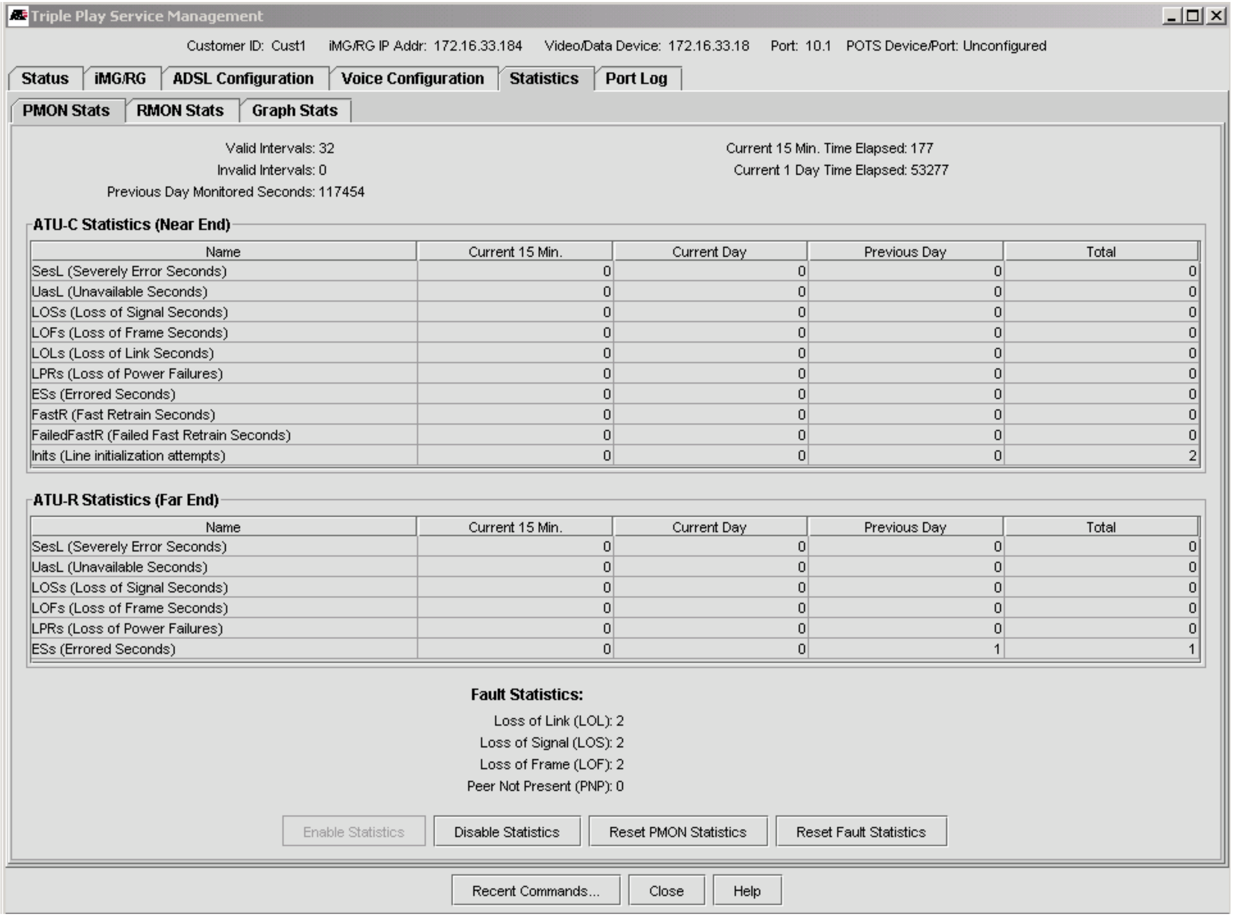
VDSL Configuration - Other Tabs

The remaining tabs follow the same concepts as the ADSL configuration. Refer to "ADSL Configuration Tab" on page 426.

14.24 Statistics Tab

The statistics tab for an overall port are shown by clicking on the Statistics tab for the port. Refer to the following figures and tables.

14.24.1 PMON Stats Tab



Customer ID: Cust1 iMG/RG IP Addr: 172.16.33.184 Video/Data Device: 172.16.33.18 Port: 10.1 POTS Device/Port: Unconfigured

Valid Intervals: 32
Invalid Intervals: 0
Previous Day Monitored Seconds: 117454
Current 15 Min. Time Elapsed: 177
Current 1 Day Time Elapsed: 53277

ATU-C Statistics (Near End)

Name	Current 15 Min.	Current Day	Previous Day	Total
SesL (Severely Error Seconds)	0	0	0	0
UasL (Unavailable Seconds)	0	0	0	0
LOSs (Loss of Signal Seconds)	0	0	0	0
LOFs (Loss of Frame Seconds)	0	0	0	0
LOLs (Loss of Link Seconds)	0	0	0	0
LPRs (Loss of Power Failures)	0	0	0	0
ESs (Errored Seconds)	0	0	0	0
FastR (Fast Retrain Seconds)	0	0	0	0
FailedFastR (Failed Fast Retrain Seconds)	0	0	0	0
Inits (Line initialization attempts)	0	0	0	2

ATU-R Statistics (Far End)

Name	Current 15 Min.	Current Day	Previous Day	Total
SesL (Severely Error Seconds)	0	0	0	0
UasL (Unavailable Seconds)	0	0	0	0
LOSs (Loss of Signal Seconds)	0	0	0	0
LOFs (Loss of Frame Seconds)	0	0	0	0
LPRs (Loss of Power Failures)	0	0	0	0
ESs (Errored Seconds)	0	0	1	1

Fault Statistics:
Loss of Link (LOL): 2
Loss of Signal (LOS): 2
Loss of Frame (LOF): 2
Peer Not Present (PNP): 0

FIGURE 14-70 Statistics - PMON

The ATU-C and ATU-R statistics have the following measurements:

- Valid Intervals
- Invalid Intervals
- Previous Day Monitored Seconds
- Current 15 min. Time Elapsed
- Current 1 Day Time Elapsed

The table for each statistic type gives the count for the periods.

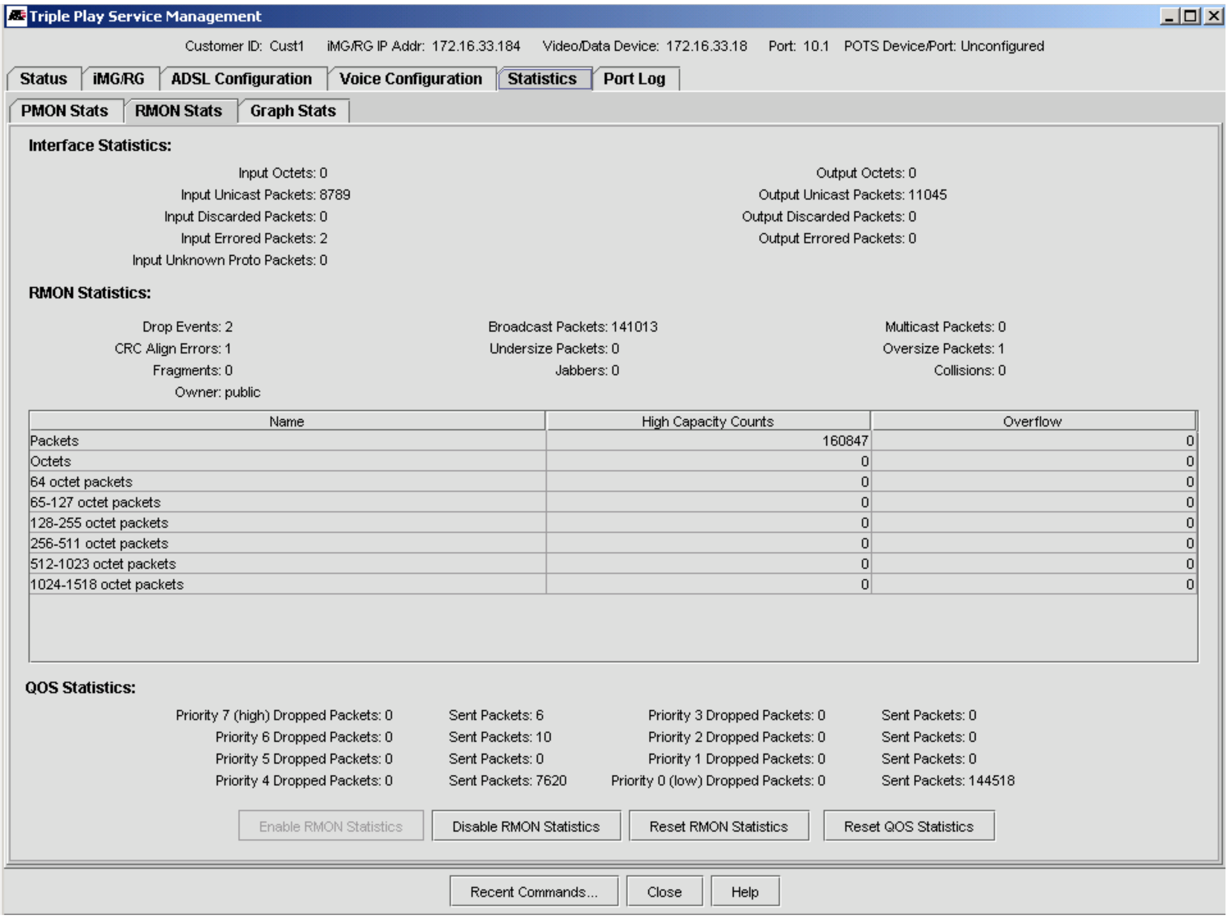
The Fault Statistics are counters, which are part of the ATN Enterprise MIB, that help to monitor the ADSL port by incrementing continuously until reset. By doing this, the history of certain events can be shown over time in order to obtain a more accurate view of what is happening with the ADSL port.

No management logs are produced with these counters, since they are cumulative, and so logs are produced for each individual event.

These counters can be reset to 0 by selecting **Reset Fault Statistics**.

Refer to the *Software Reference for iMAP Series Switches* for details about these counters.

14.24.2 RMON Stats Tab



Customer ID: Cust1 iMG/RG IP Addr: 172.16.33.184 Video/Data Device: 172.16.33.18 Port: 10.1 POTS Device/Port: Unconfigured

Interface Statistics:

Input Octets: 0
Input Unicast Packets: 8789
Input Discarded Packets: 0
Input Errored Packets: 2
Input Unknown Proto Packets: 0

Output Octets: 0
Output Unicast Packets: 11045
Output Discarded Packets: 0
Output Errored Packets: 0

RMON Statistics:

Drop Events: 2
CRC Align Errors: 1
Fragments: 0
Owner: public

Broadcast Packets: 141013
Undersize Packets: 0
Jabbers: 0

Multicast Packets: 0
Oversize Packets: 1
Collisions: 0

Name	High Capacity Counts	Overflow
Packets	160847	0
Octets	0	0
64 octet packets	0	0
65-127 octet packets	0	0
128-255 octet packets	0	0
256-511 octet packets	0	0
512-1023 octet packets	0	0
1024-1518 octet packets	0	0

QOS Statistics:

Priority 7 (high) Dropped Packets: 0 Sent Packets: 6
Priority 6 Dropped Packets: 0 Sent Packets: 10
Priority 5 Dropped Packets: 0 Sent Packets: 0
Priority 4 Dropped Packets: 0 Sent Packets: 7620

Priority 3 Dropped Packets: 0 Sent Packets: 0
Priority 2 Dropped Packets: 0 Sent Packets: 0
Priority 1 Dropped Packets: 0 Sent Packets: 0
Priority 0 (low) Dropped Packets: 0 Sent Packets: 144518

FIGURE 14-71 Statistics - PMON

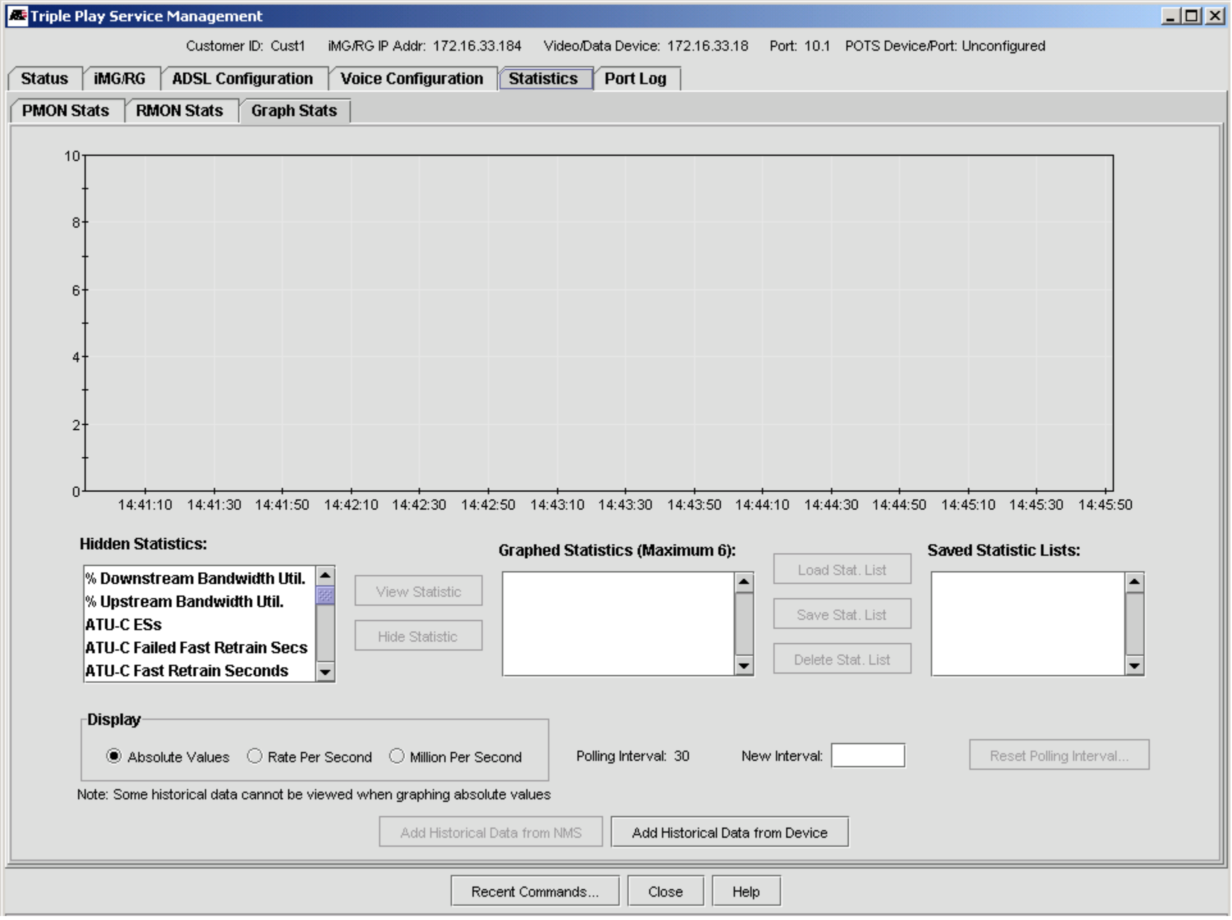
RMON Statistics deal with packet flows and highlight errors as well as overflows of packets.

The QOS Statistics are counters for each priority queue that allow the user to see the ratio of sent versus dropped packets. These are cumulative and so produce no management logs.

These counters can be reset to 0 by selecting **Reset QOS Statistics**.

Refer to the *Software Reference for iMAP Series Switches* for details about these counters.

14.24.3 Graph Stats Tab



Customer ID: Cust1 iMG/RG IP Addr: 172.16.33.184 Video/Data Device: 172.16.33.18 Port: 10.1 POTS Device/Port: Unconfigured

% Downstream Bandwidth Util.
% Upstream Bandwidth Util.
ATU-C ESs
ATU-C Failed Fast Retrain Secs
ATU-C Fast Retrain Seconds

● Absolute Values ○ Rate Per Second ○ Million Per Second

Polling Interval: 30

Note: Some historical data cannot be viewed when graphing absolute values

FIGURE 14-72 Statistics - Graph Stats

TABLE 14-29 Stats Graph Tab

Field/Button	Description
Hidden Statistics:	Statistics not added to the resulting graph
View Statistic:	Enabled when a statistic is chosen form Hidden Statistics, clicking this button adds it to the graph/
Hide Statistic:	Enabled when a statistic is chosen form Graphed Statistics, clicking this button deletes it from the graph/
Display	The attribute that controls the display: - Absolute Values - Rate Per Second - Million Per Second
Polling Interval:	Current Polling Interval in seconds
New Interval:	Sets a new interval for polling. This is set with the **Reset Polling Interval** button.

TABLE 14-29 Stats Graph Tab

Field/Button	Description
Add Historical Data from NMS:	Adds the data collected previously from NMS port management
Add Historical Data from Device:	Adds the data collected previously (buckets) from the device

14.25 Port Log Tab

Selecting the **Port Log** tab invokes a table that lists all the port-related management logs that have been generated. Refer to previous sections on the port log tab. ("ADSL Port - Port Log Tab)" on page 444, "POTS Port (Port Log Tab)" on page 456)

For a description of management logs and the meaning of fields, refer to the iMAP Log / Troubleshooting Manual.

14.26 DHCP Tab

For each port configuration tab, there is a DHCP sub-tab that supplies:

- DHCP statistics
- ability to associate a DHCP Relay instance to the port
- ability to set to ON or OFF DHCP Filtering and Ageing
- a table that shows the MAC address, VID and IP address association.

You can also clear the statistics (Reset Counters).

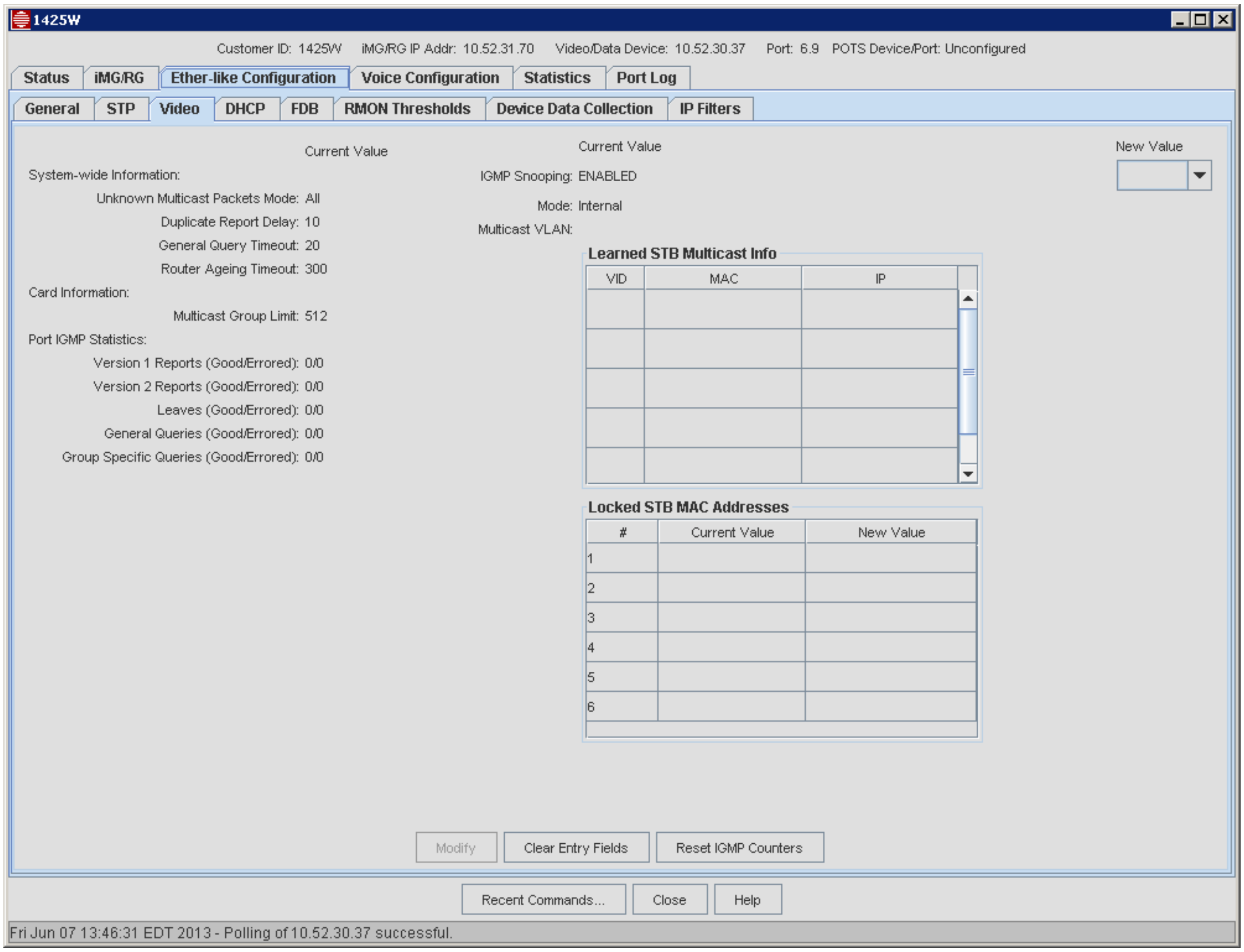
Note: *Select and change the DHCP Relay instance with care. Refer to the Software Reference for iMAP Series Switches for details on DHCP Relay, especially the difference between DHCP Relay and DHCO Snooping.*

14.27 FDB Tab

For each port configuration tab, there is an Forwarding Database (FDB) sub-tab that shows the current VLAN ID (VID) and MAC address associations, as well as the status.

14.28 Video Tab

The Video tab highlights the IGMP / multicast attributes. Refer to the following figure.



Customer ID: 1425W iMG/RG IP Addr: 10.52.31.70 Video/Data Device: 10.52.30.37 Port: 6.9 POTS Device/Port: Unconfigured

Current Value

System-wide Information:
Unknown Multicast Packets Mode: All
Duplicate Report Delay: 10
General Query Timeout: 20
Router Ageing Timeout: 300
Card Information:
Multicast Group Limit: 512
Port IGMP Statistics:
Version 1 Reports (Good/Errored): 0/0
Version 2 Reports (Good/Errored): 0/0
Leaves (Good/Errored): 0/0
General Queries (Good/Errored): 0/0
Group Specific Queries (Good/Errored): 0/0

Current Value
IGMP Snooping: ENABLED
Mode: Internal
Multicast VLAN:

New Value

Learned STB Multicast Info

VID	MAC	IP

Locked STB MAC Addresses

#	Current Value	New Value
1		
2		
3		
4		
5		
6		

Fri Jun 07 13:46:31 EDT 2013 - Polling of 10.52.30.37 successful.

FIGURE 14-73 Video Tab

TABLE 14-30 Video Tab

Field/Button	Description
System-wide Information	These are the IGMP attributes that have been set for the device. Unknown Multicast Packets Mode: Supported on iMAP 9810 and SBx3100 devices. Values are as follows: • iMAP devices running software release 17.0 and higher and SBx3100 devices running software release 17.l and higher: All, None or Control Packets Only • iMAP and SBx3100 devices running software release 16.x and lower: Drop or Flood
Card Information	The attributes for the ADSL/VDSL card, such as the Multicast Group Limit for iMAP devices. The Multicast Group Limit display is not present for SBx3100 devices running software release 17.x.x or higher.
Port IGMP Statistics	The good vs. errored number of IGMP Reports/Leaves/Queries for the port
IGMP Snooping	Whether IGMP is enabled on the port. For devices running software release 17.x.x or higher, IGMP must be enabled directly on individual VLANs.
Mode	The type of IGMP snooping to perform (Internal, External, MCPassthrough).

TABLE 14-30 Video Tab (Continued)

Field/Button	Description
Multicast VLANs	VLANs that are currently carrying multicast traffic - This is included in the l;earned STB Multicast Info table.
Multicast IP Addresses	The IP addresses being used for the multicast traffic.
Learned STB Multicast Info	VID - The multicast VLAN MAC - The STB MAC Addresses that were learned and are in the FDB IP - The IP addresses being used for the multicast traffic Note: These three attributes are placed in a table to allow the user to see the association between a VLAN ID, MAC address, and its associated IP addresses.
Locked STB MAC Address:	The set of unicast MAC addresses associated with this port. The **New Value** pull-down allows the user to enter a new valid unicast address. This will overwrite a Current Value if it exists. The Remove option removes the current value and leaves the current Value field blank. Note that several changes (add, change, remove) can be done for the MAC address rows. These changes are activated when the **Modify** button is pressed.
Clear Entry Fields	Clear any fields that have been datafilled but not yet Modified
Reset IGMP Counters	Enabled if the port is in an Administrative State of DOWN, enables the port and so brings the Administrative State to UP. If possible (for example, the card must be enabled), the Operational State will change to UP.

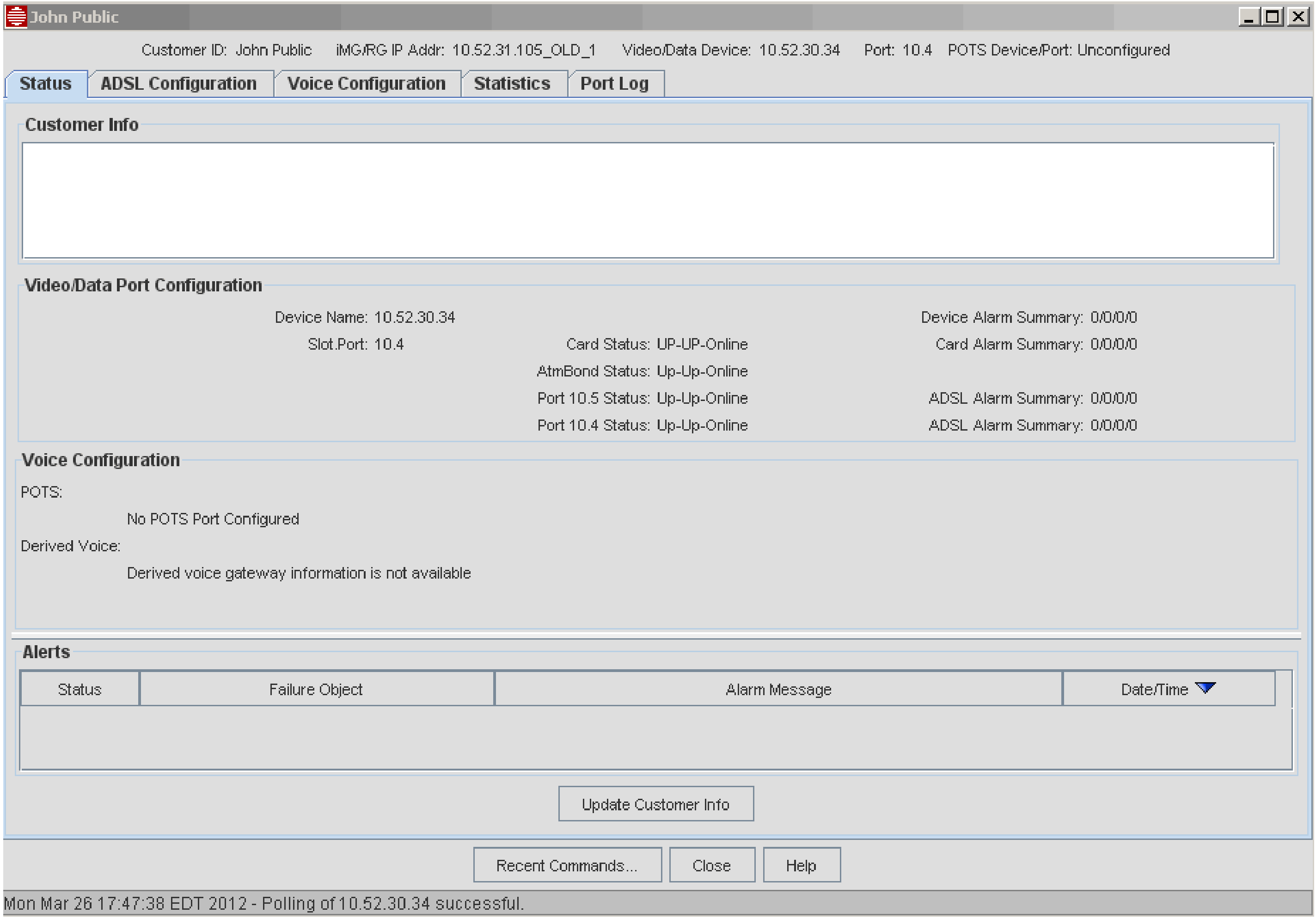
14.29 ATM Bonding

For ATM Bonding, the Service Management Form allows the user to add and remove ports.

Note: To create the ATM Bonding Group, the user should create an ATM Bonding Profile, and then use that Profile as part of provisioning with the Triple Play form. Refer to "Provisioning for ADSL G.Bond" on page 401. The result should be an ATM Bonding Group that contains all of its members.

14.29.1 Status

The status tab includes the status of the ATM Bond as well as the associated ports. Refer to the following figure.



John Public

Customer ID: John Public iMG/RG IP Addr: 10.52.31.105_OLD_1 Video/Data Device: 10.52.30.34 Port: 10.4 POTS Device/Port: Unconfigured

Customer Info

Video/Data Port Configuration

Device Name: 10.52.30.34
Slot.Port: 10.4
Card Status: UP-UP-Online
AtmBond Status: Up-Up-Online
Port 10.5 Status: Up-Up-Online
Port 10.4 Status: Up-Up-Online
Device Alarm Summary: 0/0/0/0
Card Alarm Summary: 0/0/0/0
ADSL Alarm Summary: 0/0/0/0
ADSL Alarm Summary: 0/0/0/0

Voice Configuration

POTS:
No POTS Port Configured
Derived Voice:
Derived voice gateway information is not available

Alerts

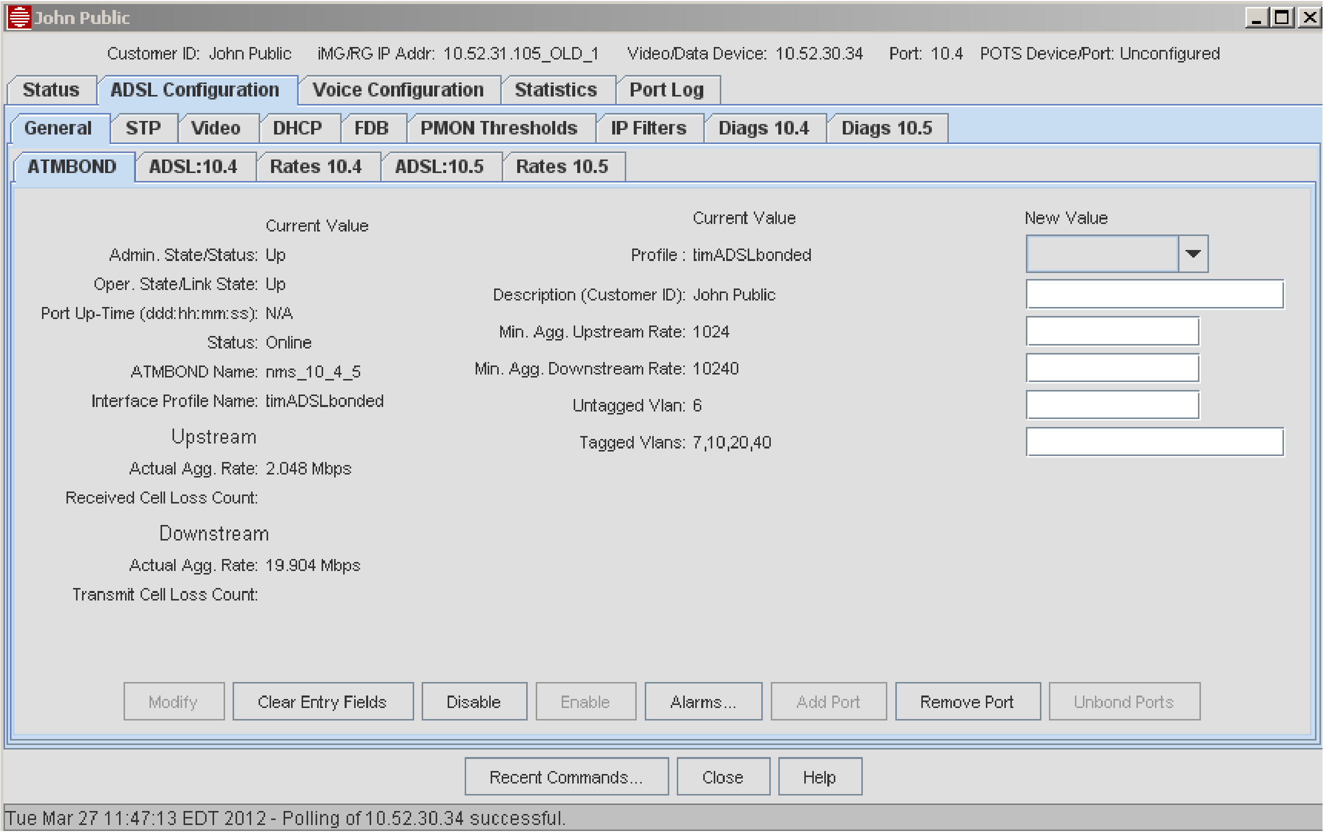
Status	Failure Object	Alarm Message	Date/Time

Mon Mar 26 17:47:38 EDT 2012 - Polling of 10.52.30.34 successful.

FIGURE 14-74 Status Tab for ATM Bond

14.29.2 Bonding Group - Viewing and Changing the Bonding Configuration

The General subtab for ATM Bonded ports gives information on both the ATM Bond and the ADSL members. Refer to the following figure.



Customer ID: John Public iMG/RG IP Addr: 10.52.31.105_OLD_1 Video/Data Device: 10.52.30.34 Port: 10.4 POTS Device/Port: Unconfigured

	Current Value
Admin. State/Status:	Up
Oper. State/Link State:	Up
Port Up-Time (ddd:hh:mm:ss):	N/A
Status:	Online
ATMBOND Name:	nms_10_4_5
Interface Profile Name:	timADSLbonded
Upstream	
Actual Agg. Rate:	2.048 Mbps
Received Cell Loss Count:	
Downstream	
Actual Agg. Rate:	19.904 Mbps
Transmit Cell Loss Count:	

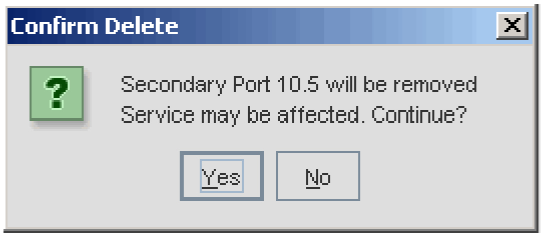
	Current Value	New Value
Profile :	timADSLbonded	
Description (Customer ID):	John Public	
Min. Agg. Upstream Rate:	1024	
Min. Agg. Downstream Rate:	10240	
Untagged Vlan:	6	
Tagged Vlans:	7,10,20,40	

Tue Mar 27 11:47:13 EDT 2012 - Polling of 10.52.30.34 successful.

FIGURE 14-75 ATMBOND Tab

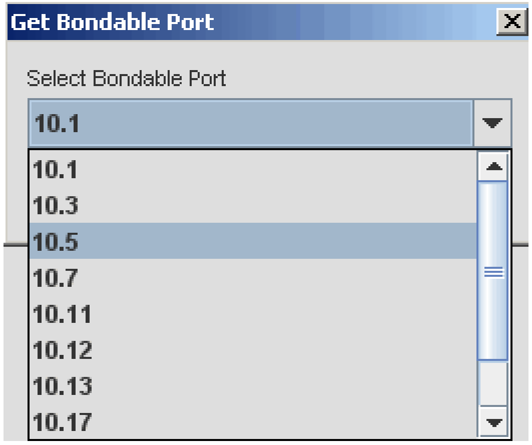
From this tab it is possible to enable and disable the ATM Bonding group, as well as add and remove ports to the bond. The available options are:

- **Remove Port** - This allows you to remove the secondary port from the ATM Bonding Group. In the **Confirm Delete** warning, selecting **Yes** drives both the Admin State and the Operational state of the Bonding group to Down.



Secondary Port 10.5 will be removed
Service may be affected. Continue?

- **Add Port** - This retrieves all ports that are not provisioned with a customer (no Customer ID) and opens a window to allow adding another port to the group. You should select a port that has the same settings as the principle port (which uses the settings of a bonded Profile). Once the port is added, the port will go to Up-Up. Click **Enable** to enable the modified group.



Get Bondable Port

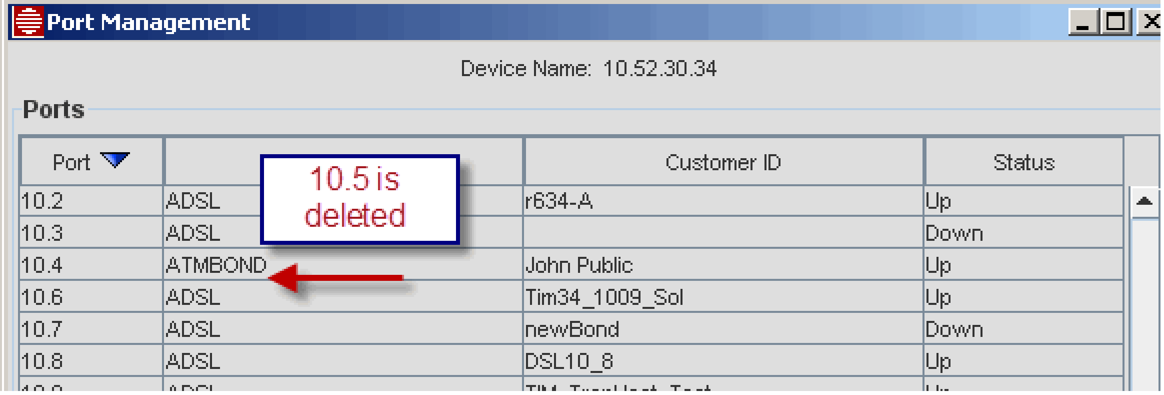
Select Bondable Port

10.1

- 10.1
- 10.3
- 10.5
- 10.7
- 10.11
- 10.12
- 10.13
- 10.17

FIGURE 14-76 Selecting a Port to add to Bonding Group

- **Enable** - If the group is disabled, the **Enable** button is available. **Enable** drives the ports to an Operational Status of UP, and then sets the ATM Bonding Group to UP. At this point Port Management will show the root port as Type ATMBOND and the secondary port will no longer be in the port list.



Port Management

Device Name: 10.52.30.34

Ports

Port		Customer ID	Status
10.2	ADSL	r634-A	Up
10.3	ADSL		Down
10.4	ATMBOND	John Public	Up
10.6	ADSL	Tim34_1009_Sol	Up
10.7	ADSL	newBond	Down
10.8	ADSL	DSL10_8	Up

10.5 is deleted

FIGURE 14-77 Port is Added to Bonding Group and Deleted in Port Management Table

Note: *Removing a port from an ATM Bonding Group does not change the ATMBOND Name listed on the ATMBOND tab. This name is set during the original bonding provisioning and does not change when the ATM Bonding Group is modified.*

14.29.3 Bonding Group - Viewing and Changing the Port Configuration

Each port in the bonding group has its own Status tab and Rates tab. For the Status tab there are the following options:

- **Disable Port** - From the Port tab, this disassociates the port from the Bonding group. If one port of the two members is disabled, the ATMBOND state goes to Up-Up-Degraded, but the group will continue to be in an UP state. Note that in this scenario the root port could be disabled and the Bonding Group would remain in service (with a Status of Degraded).
- **Enable Port** - This associates the port to the bonding group, and once the port is in an Up-Up state, it will join the Bonding group.

14.29.4 De-provision a Port from the Bonding Group

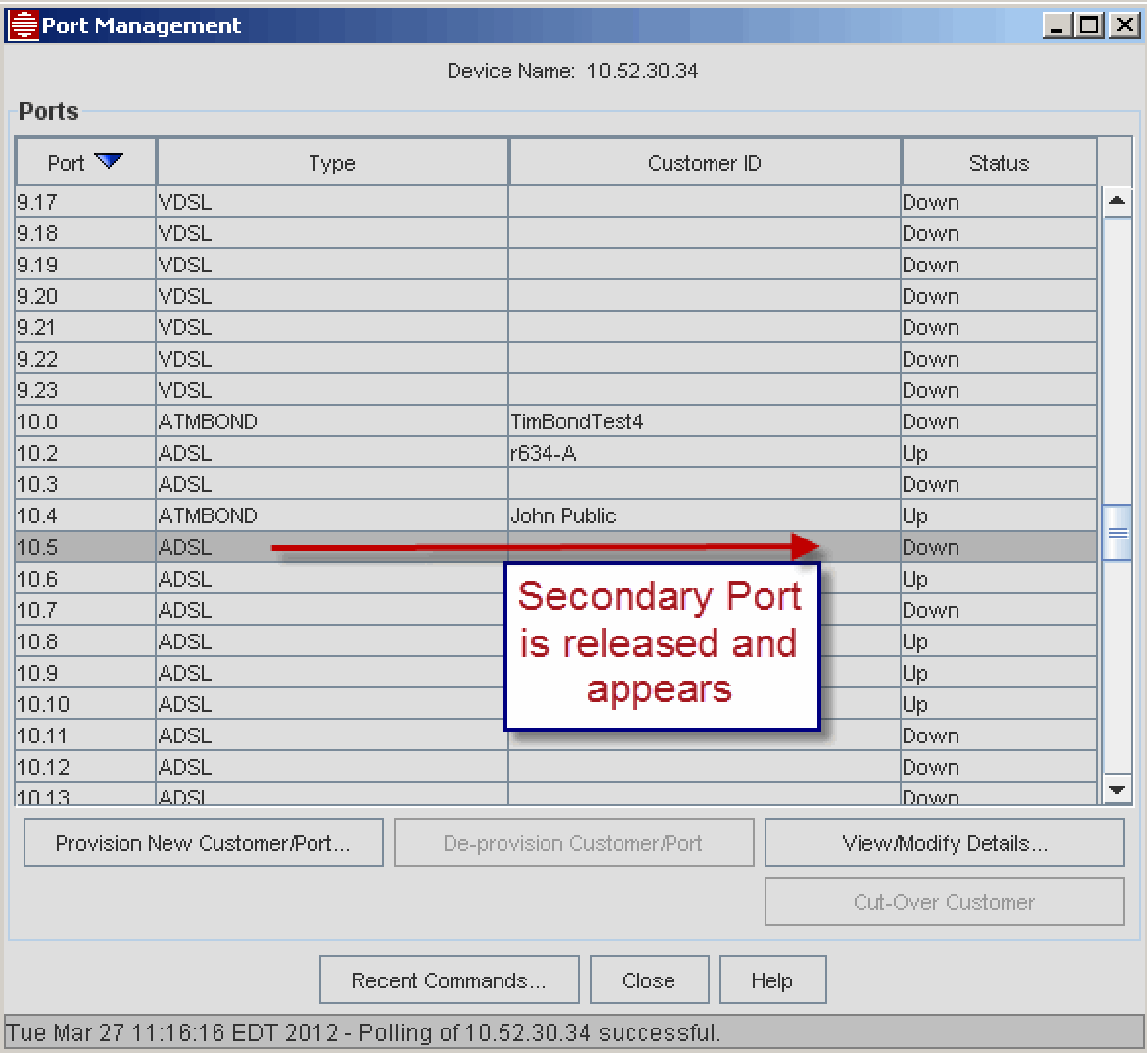
To remove the secondary port from the Group so that it can be used in other applications, use these steps:

1. In the ATM Bond Tab of the Service Management form, select **Remove Port**.
2. Notice that in the Port Management table, the secondary port reappears.

3. In the Port Management table, select the now freed secondary port and select **View/Modify Details**.
4. In the ADSL tab, select **Disable**.

At this point, the port is released from the Group and is added back to the Port Management table, **retaining all of its previous settings**.

Note: *The port retains all of its settings, and so you will need to change the settings (preferably through a Profile), if another application requires different settings.*



Device Name: 10.52.30.34

Port	Type	Customer ID	Status
9.17	VDSL		Down
9.18	VDSL		Down
9.19	VDSL		Down
9.20	VDSL		Down
9.21	VDSL		Down
9.22	VDSL		Down
9.23	VDSL		Down
10.0	ATMBOND	TimBondTest4	Down
10.2	ADSL	r634-A	Up
10.3	ADSL		Down
10.4	ATMBOND	John Public	Up
10.5	ADSL		Down
10.6	ADSL		Up
10.7	ADSL		Down
10.8	ADSL		Up
10.9	ADSL		Up
10.10	ADSL		Up
10.11	ADSL		Down
10.12	ADSL		Down
10.13	ADSL		Down

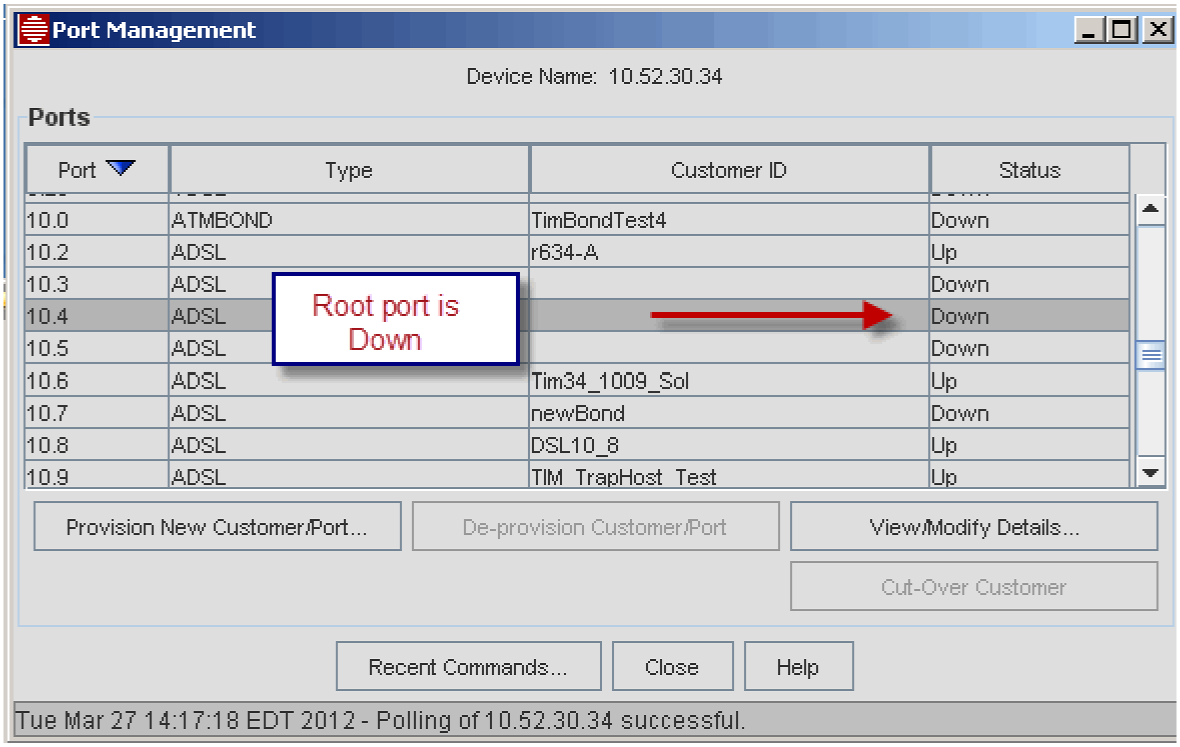
Secondary Port is released and appears

Tue Mar 27 11:16:16 EDT 2012 - Polling of 10.52.30.34 successful.

FIGURE 14-78 Secondary Port is Released, can be Provisioned for other Applications

14.29.5 Destroying the ATM Bonding Group

To destroy the ATM Bonding Group, go to the primary port in the Port Management table. Select **De-provision Customer Port**, then choose **Select All** and **De-provision**. The Root port goes to Down and can now be provisioned for other applications. Refer to the following figure.



Device Name: 10.52.30.34

Port	Type	Customer ID	Status
10.0	ATMBOND	TimBondTest4	Down
10.2	ADSL	r634-A	Up
10.3	ADSL		Down
10.4	ADSL		Down
10.5	ADSL		Down
10.6	ADSL	Tim34_1009_Sol	Up
10.7	ADSL	newBond	Down
10.8	ADSL	DSL10_8	Up
10.9	ADSL	TIM_TrapHost_Test	Up

Root port is Down

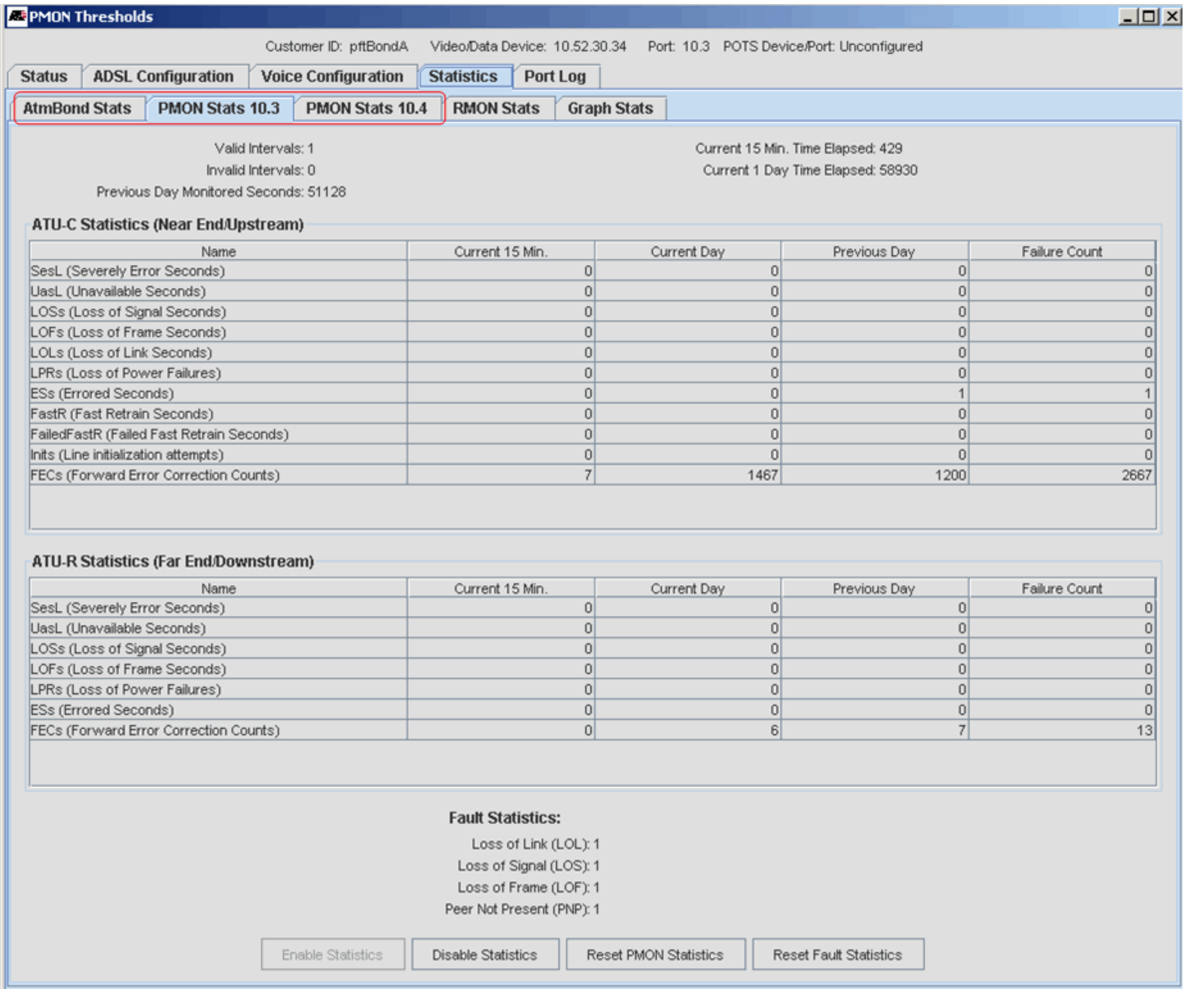
Tue Mar 27 14:17:18 EDT 2012 - Polling of 10.52.30.34 successful.

FIGURE 14-79 ATM Bonding Group is Destroyed

Note: *If the user selects the Provision New Customer/Port, the system will have a message window that it is selecting all bondable ports. This is only for use if the port is to be part of an ATM Bonding Group; for other applications it is not needed.*

14.29.6 PMON Thresholds

AtmBond statistics are on a new tab. PMONs can be set for the for each ADSL line. RMONs are tied to the Bond interface. PMON statistics can be collected for each Interface



Customer ID: pftBondA Video/Data Device: 10.52.30.34 Port: 10.3 POTS Device/Port: Unconfigured

Valid Intervals: 1
Invalid Intervals: 0
Previous Day Monitored Seconds: 51128

Current 15 Min. Time Elapsed: 429
Current 1 Day Time Elapsed: 58930

ATU-C Statistics (Near End/Upstream)

Name	Current 15 Min.	Current Day	Previous Day	Failure Count
SesL (Severely Error Seconds)	0	0	0	0
UasL (Unavailable Seconds)	0	0	0	0
LOSs (Loss of Signal Seconds)	0	0	0	0
LOFs (Loss of Frame Seconds)	0	0	0	0
LOLs (Loss of Link Seconds)	0	0	0	0
LPRs (Loss of Power Failures)	0	0	0	0
ESs (Errored Seconds)	0	0	1	1
FastR (Fast Retrain Seconds)	0	0	0	0
FailedFastR (Failed Fast Retrain Seconds)	0	0	0	0
Inits (Line initialization attempts)	0	0	0	0
FECs (Forward Error Correction Counts)	7	1467	1200	2667

ATU-R Statistics (Far End/Downstream)

Name	Current 15 Min.	Current Day	Previous Day	Failure Count
SesL (Severely Error Seconds)	0	0	0	0
UasL (Unavailable Seconds)	0	0	0	0
LOSs (Loss of Signal Seconds)	0	0	0	0
LOFs (Loss of Frame Seconds)	0	0	0	0
LPRs (Loss of Power Failures)	0	0	0	0
ESs (Errored Seconds)	0	0	0	0
FECs (Forward Error Correction Counts)	0	6	7	13

Fault Statistics:

Loss of Link (LOL): 1
Loss of Signal (LOS): 1
Loss of Frame (LOF): 1
Peer Not Present (PNP): 1

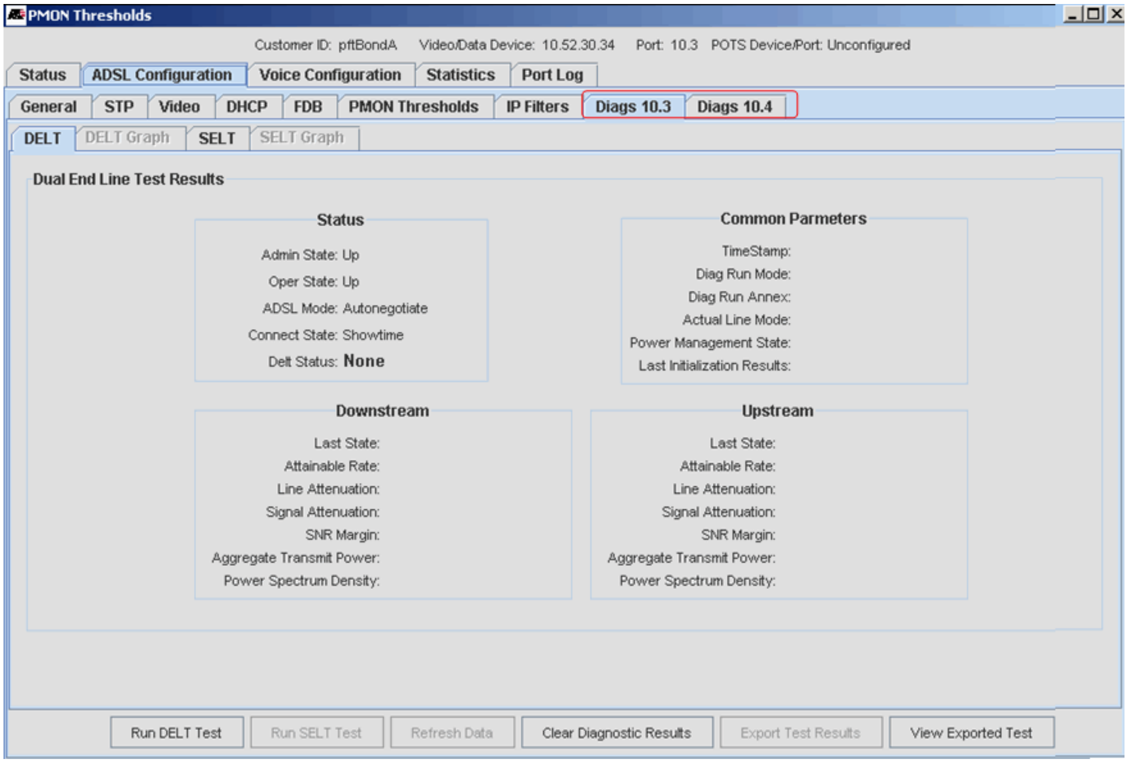
FIGURE 14-80 ATMBOND Statistics

14.29.7 Diagnostics

DELT (Dual End Line Test) and SELT (Single End Line Test) can be run on each ADSL port when they are in the appropriate state:

- For DELT that is Up/Up/Showtime
- For SELT Up/Down

Note: These tests may not actually work with the particular modems being used



Customer ID: pftBondA Video/Data Device: 10.52.30.34 Port: 10.3 POTS Device/Port: Unconfigured

Dual End Line Test Results

Status

Admin State: Up
Oper State: Up
ADSL Mode: Autonegotiate
Connect State: Showtime
Delt Status: None

Common Parmeters

TimeStamp:
Diag Run Mode:
Diag Run Annex:
Actual Line Mode:
Power Management State:
Last Initialization Results:

Downstream

Last State:
Attainable Rate:
Line Attenuation:
Signal Attenuation:
SNR Margin:
Aggregate Transmit Power:
Power Spectrum Density:

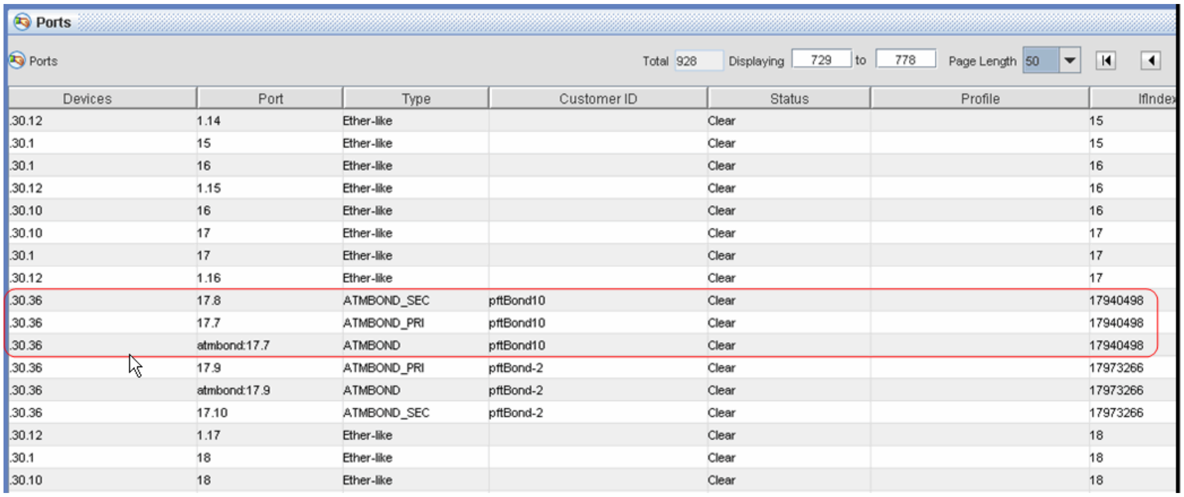
Upstream

Last State:
Attainable Rate:
Line Attenuation:
Signal Attenuation:
SNR Margin:
Aggregate Transmit Power:
Power Spectrum Density:

FIGURE 14-81 ATMBOND Diags

14.29.8 Network Inventory - Customer Ports

For ATMBOND ports a Managed Object is created to represent the ATMBOND. Its port number is preceded by ‘atmbond:”, and it has the same number as its primary port. Its type is “ATMBOND”. The primary ADSL ports type is changed to “ATMBOND-PRI” and each secondary ADSL port to “ATMBOND-SEC”. All Managed Objects will share the same CustomerID and IfIndex. The ifIndex is for the Ethernet Interface that they all share



Total 928 Displaying 729 to 778 Page Length 50

Devices	Port	Type	Customer ID	Status	Profile	IfIndex
.30.12	1.14	Ether-like		Clear		15
.30.1	15	Ether-like		Clear		15
.30.1	16	Ether-like		Clear		16
.30.12	1.15	Ether-like		Clear		16
.30.10	16	Ether-like		Clear		16
.30.10	17	Ether-like		Clear		17
.30.1	17	Ether-like		Clear		17
.30.12	1.16	Ether-like		Clear		17
.30.36	17.8	ATMBOND_SEC	pftBond10	Clear		17940498
.30.36	17.7	ATMBOND_PRI	pftBond10	Clear		17940498
.30.36	atmbond:17.7	ATMBOND	pftBond10	Clear		17940498
.30.36	17.9	ATMBOND_PRI	pftBond-2	Clear		17973266
.30.36	atmbond:17.9	ATMBOND	pftBond-2	Clear		17973266
.30.36	17.10	ATMBOND_SEC	pftBond-2	Clear		17973266
.30.12	1.17	Ether-like		Clear		18
.30.1	18	Ether-like		Clear		18
.30.10	18	Ether-like		Clear		18

FIGURE 14-82 Network Inventory for ATMBOND

14.30 STP Tab

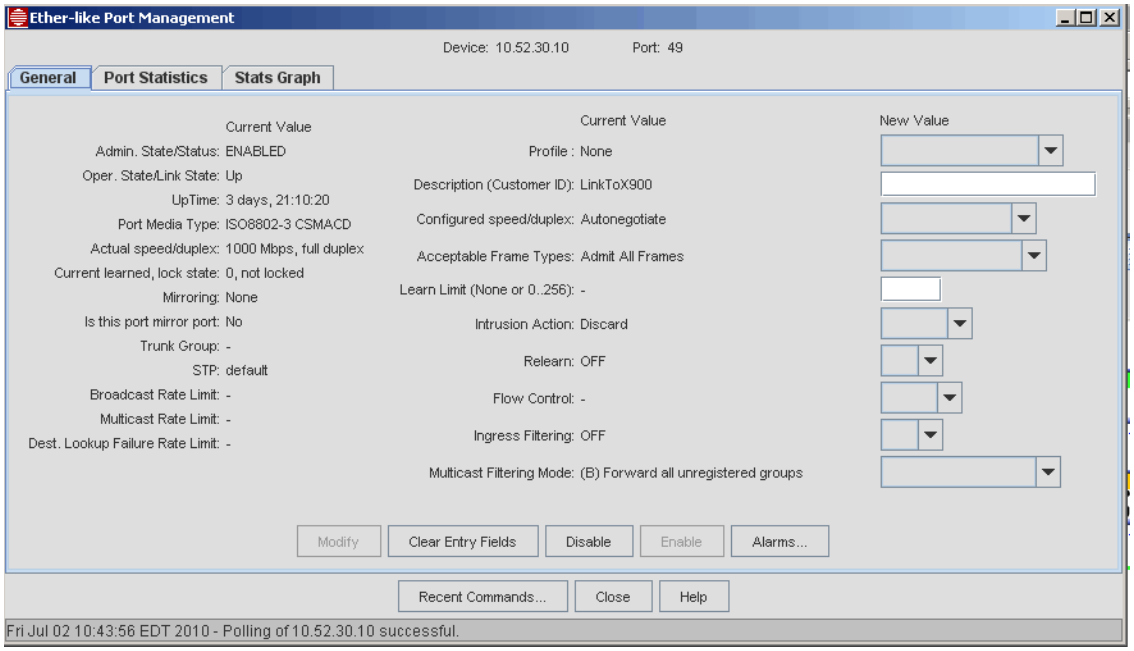
For each port configuration tab, there is an STP tab or sub-tab that shows the current STP attributes. Refer to the *Software Reference for iMAP Series Switches* for details.

15. Port Management - non-iMAP Devices

Port management is provided for the Rapier and Switchblade devices, including the the 8700 and 9800 series.

Note: For complete information on Rapier and Switchblade devices, go to http://www.alliedtelesis.co.nz/documentation/.

15.1 Rapier/Switchblade Devices



Device: 10.52.30.10 Port: 49

Current Value
Admin. State/Status: ENABLED
Oper. State/Link State: Up
UpTime: 3 days, 21:10:20
Port Media Type: ISO8802-3 CSMACD
Actual speed/duplex: 1000 Mbps, full duplex
Current learned, lock state: 0, not locked
Mirroring: None
Is this port mirror port: No
Trunk Group: -
STP: default
Broadcast Rate Limit: -
Multicast Rate Limit: -
Dest. Lookup Failure Rate Limit: -

Current Value / New Value
Profile : None
Description (Customer ID): LinkToX900
Configured speed/duplex: Autonegotiate
Acceptable Frame Types: Admit All Frames
Learn Limit (None or 0..256): -
Intrusion Action: Discard
Relearn: OFF
Flow Control: -
Ingress Filtering: OFF
Multicast Filtering Mode: (B) Forward all unregistered groups

Fri Jul 02 10:43:56 EDT 2010 - Polling of 10.52.30.10 successful.

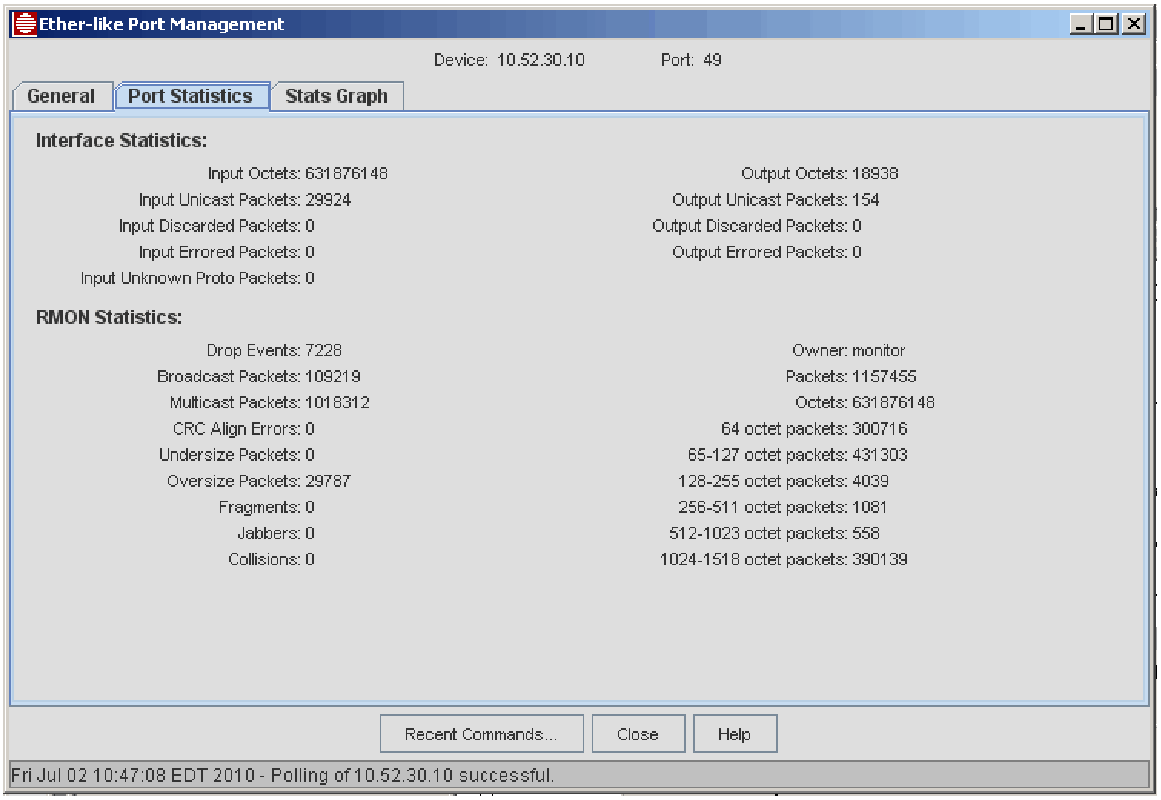
FIGURE 15-1 Ether like Port Management (Rapier Device) - General Tab

TABLE 15-1 Ether-like Port Management for Rapier and SwitchBlade Devices - General Tab

Field/Button	Description
Admin. State/Status:	The Administrative State can be controlled and determines the Operational State. *Note: The possible values are ENABLED/DISABLED (rather than the Up/Down for iMAP devices).*
Oper. State/Link State:	The ability of the port to provide service. The Administrative State must be Up and then the system determines if the port can provide service. *Note: There is no Status field as in iMAP devices. Only the Up/Down values are used.*
Other fields	For details on all other fields refer to Allied Telesis documentation.
Modify	Enables the any changes have been made to the settings, makes them

TABLE 15-1 Ether-like Port Management for Rapier and SwitchBlade Devices - General Tab

Field/Button	Description
Disable	Disable the port (after a confirmation window). This makes the overall state DOWN.
Enable	Enable the port. This makes the overall STATE UP if the port can be brought into service.
Alarms	Brings up the Alarm view for the selected port.
Clear Entry Fields	Clears the writable fields of any values.



Device: 10.52.30.10 Port: 49

Interface Statistics:

Input Octets: 631876148
Input Unicast Packets: 29924
Input Discarded Packets: 0
Input Errored Packets: 0
Input Unknown Proto Packets: 0

Output Octets: 18938
Output Unicast Packets: 154
Output Discarded Packets: 0
Output Errored Packets: 0

RMON Statistics:

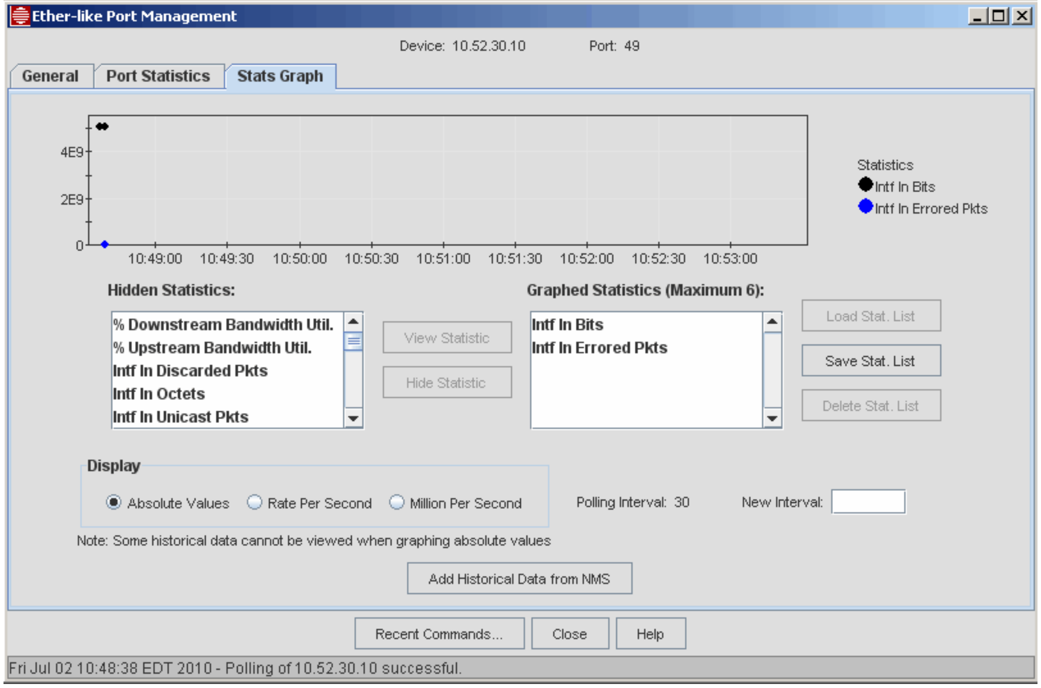
Drop Events: 7228
Broadcast Packets: 109219
Multicast Packets: 1018312
CRC Align Errors: 0
Undersize Packets: 0
Oversize Packets: 29787
Fragments: 0
Jabbers: 0
Collisions: 0

Owner: monitor
Packets: 1157455
Octets: 631876148
64 octet packets: 300716
65-127 octet packets: 431303
128-255 octet packets: 4039
256-511 octet packets: 1081
512-1023 octet packets: 558
1024-1518 octet packets: 390139

Fri Jul 02 10:47:08 EDT 2010 - Polling of 10.52.30.10 successful.

FIGURE 15-2 Ether like Port Management (Rapier Device) - Port Statistics Tab

This form lists the standard RMON statistics.



Ether-like Port Management

Device: 10.52.30.10 Port: 49

Hidden Statistics:

% Downstream Bandwidth Util.
% Upstream Bandwidth Util.
Intf In Discarded Pkts
Intf In Octets
Intf In Unicast Pkts

Graphed Statistics (Maximum 6):

Intf In Bits
Intf In Errored Pkts

Display

● Absolute Values ○ Rate Per Second ○ Million Per Second

Polling Interval: 30 New Interval:

Note: Some historical data cannot be viewed when graphing absolute values

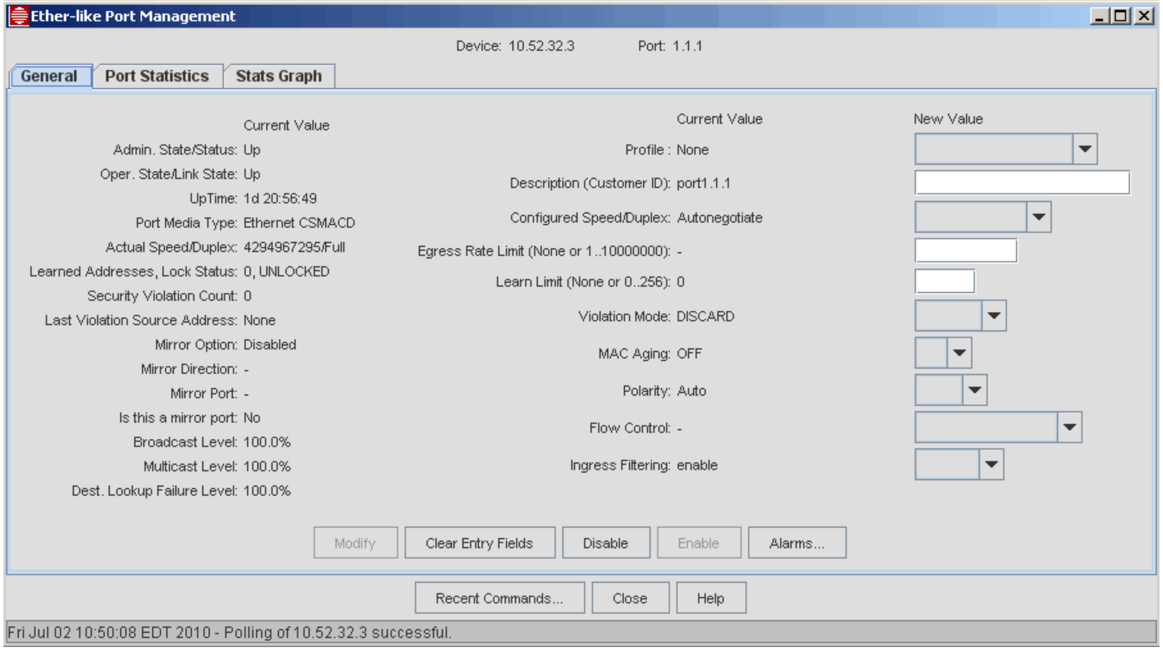
Fri Jul 02 10:48:38 EDT 2010 - Polling of 10.52.30.10 successful.

FIGURE 15-3 Ether like Port Management (Rapier Device) - Stats Graph Tab

TABLE 15-2 Provision Port Form for Port Management (Rapier Device) - Stats Graph Tab

Field/Button	Description
Hidden Statistics:	Statistics not added to the resulting graph
View Statistic:	Enabled when a statistic is chosen form Hidden Statistics, clicking this button adds it to the graph/
Hide Statistic:	Enabled when a statistic is chosen form Graphed Statistics, clicking this button deletes it from the graph/
Display	The attribute that controls the display: - Absolute Values - Rate Per Second - Million Per Second
Polling Interval:	Current Polling Interval in seconds
New Interval:	Sets a new interval for polling. This is set with the **Reset Polling Interval** button.
Add Historical Data from NMS:	Adds the data collected previously from NMS port management
Add Historical Data from Device:	Adds the data collected previously (buckets) from the device

For Switchblade devices, the ether-like port attributes are similar except for the General tab. Refer to the following figure.



Device: 10.52.32.3 Port: 1.1.1

Current Value
Admin. State/Status: Up
Oper. State/Link State: Up
UpTime: 1d 20:56:49
Port Media Type: Ethernet CSMACD
Actual Speed/Duplex: 4294967295/Full
Learned Addresses, Lock Status: 0, UNLOCKED
Security Violation Count: 0
Last Violation Source Address: None
Mirror Option: Disabled
Mirror Direction: -
Mirror Port: -
Is this a mirror port: No
Broadcast Level: 100.0%
Multicast Level: 100.0%
Dest. Lookup Failure Level: 100.0%

	Current Value	New Value
Profile :	None	
Description (Customer ID):	port1.1.1	
Configured Speed/Duplex:	Autonegotiate	
Egress Rate Limit (None or 1..10000000):	-	
Learn Limit (None or 0..256):	0	
Violation Mode:	DISCARD	
MAC Aging:	OFF	
Polarity:	Auto	
Flow Control:	-	
Ingress Filtering:	enable	

Fri Jul 02 10:50:08 EDT 2010 - Polling of 10.52.32.3 successful.

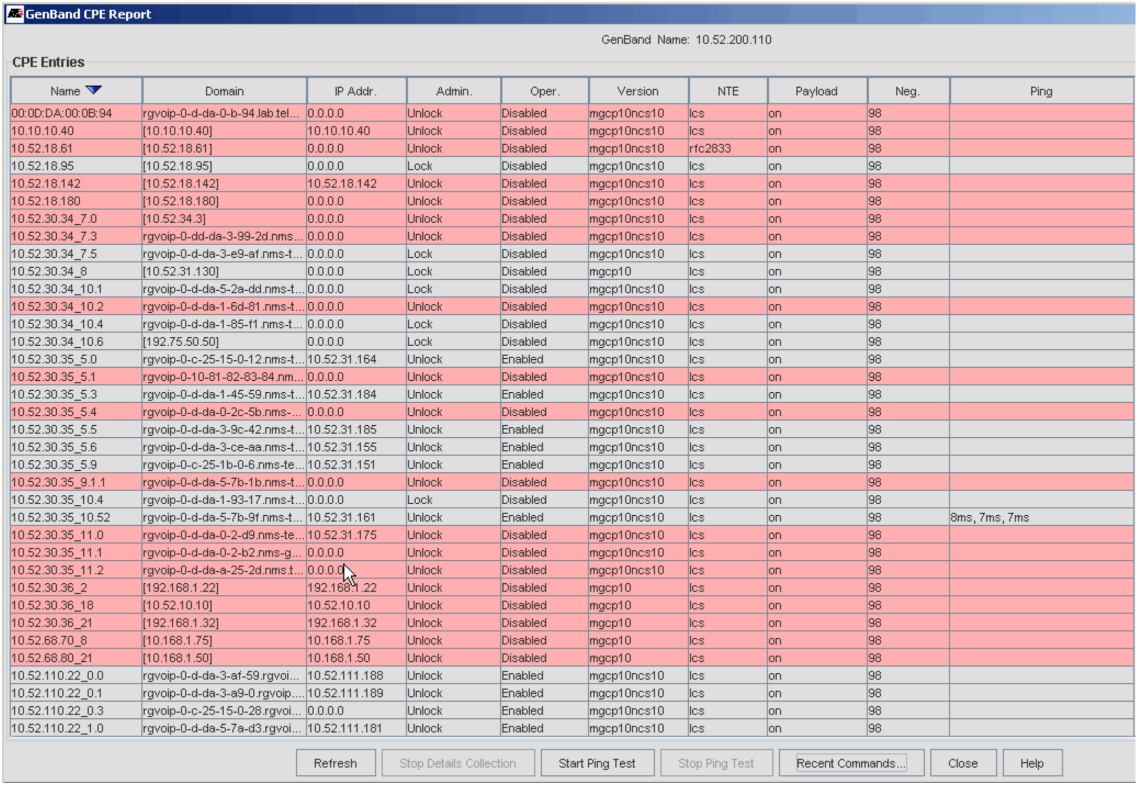
FIGURE 15-4 Ether like Port Management (SwitchBlade Device) - General Tab

Refer to Table 15-1 for a description of the main buttons. For details on all other fields refer to Allied Telesis documentation.

15.2 GenBand Reports

15.2.1 CPE Reports

This table is accessed by right clicking on the GenBand icon and choosing *Display CPE Report*. This brings up the following figure.



GenBand CPE Report

GenBand Name: 10.52.200.110

CPE Entries

Name	Domain	IP Addr.	Admin.	Oper.	Version	NTE	Payload	Neg.	Ping
00:0D:DA:00:0B:94	rgvoip-0-d-da-0-b-94.lab.tel...	0.0.0.0	Unlock	Disabled	mgcp10ncs10	lcs	on	98	
10.10.10.40	[10.10.10.40]	10.10.10.40	Unlock	Disabled	mgcp10ncs10	lcs	on	98	
10.52.18.61	[10.52.18.61]	0.0.0.0	Unlock	Disabled	mgcp10ncs10	rfc2833	on	98	
10.52.18.95	[10.52.18.95]	0.0.0.0	Lock	Disabled	mgcp10ncs10	lcs	on	98	
10.52.18.142	[10.52.18.142]	10.52.18.142	Unlock	Disabled	mgcp10ncs10	lcs	on	98	
10.52.18.180	[10.52.18.180]	0.0.0.0	Unlock	Disabled	mgcp10ncs10	lcs	on	98	
10.52.30.34_7.0	[10.52.34.3]	0.0.0.0	Unlock	Disabled	mgcp10ncs10	lcs	on	98	
10.52.30.34_7.3	rgvoip-0-dd-da-3-99-2d.nms...	0.0.0.0	Unlock	Disabled	mgcp10ncs10	lcs	on	98	
10.52.30.34_7.5	rgvoip-0-d-da-3-e9-af.nms-t...	0.0.0.0	Lock	Disabled	mgcp10ncs10	lcs	on	98	
10.52.30.34_8	[10.52.31.130]	0.0.0.0	Lock	Disabled	mgcp10	lcs	on	98	
10.52.30.34_10.1	rgvoip-0-d-da-5-2a-dd.nms-t...	0.0.0.0	Lock	Disabled	mgcp10ncs10	lcs	on	98	
10.52.30.34_10.2	rgvoip-0-d-da-1-6d-81.nms-t...	0.0.0.0	Unlock	Disabled	mgcp10ncs10	lcs	on	98	
10.52.30.34_10.4	rgvoip-0-d-da-1-85-f1.nms-t...	0.0.0.0	Lock	Disabled	mgcp10ncs10	lcs	on	98	
10.52.30.34_10.6	[192.75.50.50]	0.0.0.0	Lock	Disabled	mgcp10ncs10	lcs	on	98	
10.52.30.35_5.0	rgvoip-0-c-25-15-0-12.nms-t...	10.52.31.164	Unlock	Enabled	mgcp10ncs10	lcs	on	98	
10.52.30.35_5.1	rgvoip-0-10-81-82-83-84.nm...	0.0.0.0	Unlock	Disabled	mgcp10ncs10	lcs	on	98	
10.52.30.35_5.3	rgvoip-0-d-da-1-45-59.nms-t...	10.52.31.184	Unlock	Enabled	mgcp10ncs10	lcs	on	98	
10.52.30.35_5.4	rgvoip-0-d-da-0-2c-5b.nms-...	0.0.0.0	Unlock	Disabled	mgcp10ncs10	lcs	on	98	
10.52.30.35_5.5	rgvoip-0-d-da-3-9c-42.nms-t...	10.52.31.185	Unlock	Enabled	mgcp10ncs10	lcs	on	98	
10.52.30.35_5.6	rgvoip-0-d-da-3-ce-aa.nms-t...	10.52.31.155	Unlock	Enabled	mgcp10ncs10	lcs	on	98	
10.52.30.35_5.9	rgvoip-0-c-25-1b-0-6.nms-te...	10.52.31.151	Unlock	Enabled	mgcp10ncs10	lcs	on	98	
10.52.30.35_9.1.1	rgvoip-0-d-da-5-7b-1b.nms-t...	0.0.0.0	Unlock	Disabled	mgcp10ncs10	lcs	on	98	
10.52.30.35_10.4	rgvoip-0-d-da-1-93-17.nms-t...	0.0.0.0	Lock	Disabled	mgcp10ncs10	lcs	on	98	
10.52.30.35_10.52	rgvoip-0-d-da-5-7b-9f.nms-t...	10.52.31.161	Unlock	Enabled	mgcp10ncs10	lcs	on	98	8ms, 7ms, 7ms
10.52.30.35_11.0	rgvoip-0-d-da-0-2-d9.nms-te...	10.52.31.175	Unlock	Disabled	mgcp10ncs10	lcs	on	98	
10.52.30.35_11.1	rgvoip-0-d-da-0-2-b2.nms-g...	0.0.0.0	Unlock	Disabled	mgcp10ncs10	lcs	on	98	
10.52.30.35_11.2	rgvoip-0-d-da-a-25-2d.nms.t...	0.0.0.0	Unlock	Disabled	mgcp10ncs10	lcs	on	98	
10.52.30.36_2	[192.168.1.22]	192.168.1.22	Unlock	Disabled	mgcp10	lcs	on	98	
10.52.30.36_18	[10.52.10.10]	10.52.10.10	Unlock	Disabled	mgcp10	lcs	on	98	
10.52.30.36_21	[192.168.1.32]	192.168.1.32	Unlock	Disabled	mgcp10	lcs	on	98	
10.52.68.70_8	[10.168.1.75]	10.168.1.75	Unlock	Disabled	mgcp10	lcs	on	98	
10.52.68.80_21	[10.168.1.50]	10.168.1.50	Unlock	Disabled	mgcp10	lcs	on	98	
10.52.110.22_0.0	rgvoip-0-d-da-3-af-59.rgvoi...	10.52.111.188	Unlock	Enabled	mgcp10ncs10	lcs	on	98	
10.52.110.22_0.1	rgvoip-0-d-da-3-a9-0.rgvoip....	10.52.111.189	Unlock	Enabled	mgcp10ncs10	lcs	on	98	
10.52.110.22_0.3	rgvoip-0-c-25-15-0-28.rgvoi...	0.0.0.0	Unlock	Enabled	mgcp10ncs10	lcs	on	98	
10.52.110.22_1.0	rgvoip-0-d-da-5-7a-d3.rgvoi...	10.52.111.181	Unlock	Enabled	mgcp10ncs10	lcs	on	98	

FIGURE 15-5 GenBand CPE Report

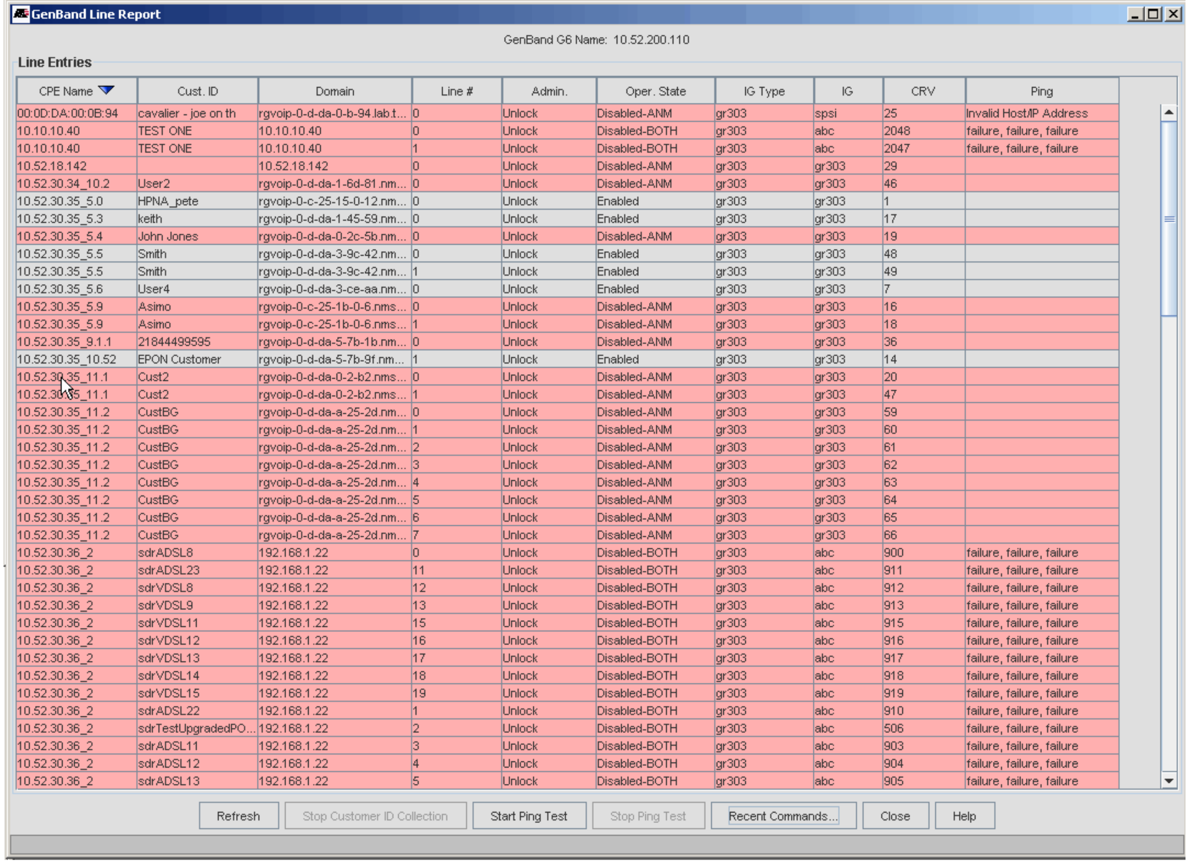
This table provides the values for the GenBand connection to the CPE and includes:

- CPE Name - When provisioned by the NMS, includes the IP address of the associated iMAP and port.
- Domain - This is explained in section 7, and must be provisioned for voice service to work. If the value is only an IP address, the value has been manually configured.
- IP Addr. - This is the voice IP address of the iMG
- Admin - This controls whether the CPE can be brought into service.
- Oper. - The actual state of the CPE. It can be Enabled only if the Oper. State is Unlock
- Version - The mgcp protocol version
- NTE - Whether the GenBand uses inband (lcs) or out-of-band (ncs) control of mgcp. This is usually lcs.
- Ping results - This is the result of selecting the Start Ping Test on a row

15.2.2 Line Reports

This table is accessed by right clicking on the GenBand icon and choosing *Display Line Report*. This brings up the following figure.

This table provides information down to the individual connection and also has a ping feature. Refer to the following figure.



GenBand G6 Name: 10.52.200.110

Line Entries

CPE Name	Cust. ID	Domain	Line #	Admin.	Oper. State	IG Type	IG	CRV	Ping
00:0D:DA:00:0B:94	cavalier - joe on th	rgvoip-0-d-da-0-b-94.lab.t...	0	Unlock	Disabled-ANM	gr303	spsi	25	Invalid Host/IP Address
10.10.10.40	TEST ONE	10.10.10.40	0	Unlock	Disabled-BOTH	gr303	abc	2048	failure, failure, failure
10.10.10.40	TEST ONE	10.10.10.40	1	Unlock	Disabled-BOTH	gr303	abc	2047	failure, failure, failure
10.52.18.142		10.52.18.142	0	Unlock	Disabled-ANM	gr303	gr303	29	
10.52.30.34_10.2	User2	rgvoip-0-d-da-1-6d-81.nm...	0	Unlock	Disabled-ANM	gr303	gr303	46	
10.52.30.35_5.0	HPNA_pete	rgvoip-0-c-25-15-0-12.nm...	0	Unlock	Enabled	gr303	gr303	1	
10.52.30.35_5.3	keith	rgvoip-0-d-da-1-45-59.nm...	0	Unlock	Enabled	gr303	gr303	17	
10.52.30.35_5.4	John Jones	rgvoip-0-d-da-0-2c-5b.nm...	0	Unlock	Disabled-ANM	gr303	gr303	19	
10.52.30.35_5.5	Smith	rgvoip-0-d-da-3-9c-42.nm...	0	Unlock	Enabled	gr303	gr303	48	
10.52.30.35_5.5	Smith	rgvoip-0-d-da-3-9c-42.nm...	1	Unlock	Enabled	gr303	gr303	49	
10.52.30.35_5.6	User4	rgvoip-0-d-da-3-ce-aa.nm...	0	Unlock	Enabled	gr303	gr303	7	
10.52.30.35_5.9	Asimo	rgvoip-0-c-25-1b-0-6.nms...	0	Unlock	Disabled-ANM	gr303	gr303	16	
10.52.30.35_5.9	Asimo	rgvoip-0-c-25-1b-0-6.nms...	1	Unlock	Disabled-ANM	gr303	gr303	18	
10.52.30.35_9.1.1	21844499595	rgvoip-0-d-da-5-7b-1b.nm...	0	Unlock	Disabled-ANM	gr303	gr303	36	
10.52.30.35_10.52	EPON Customer	rgvoip-0-d-da-5-7b-9f.nm...	1	Unlock	Enabled	gr303	gr303	14	
10.52.30.35_11.1	Cust2	rgvoip-0-d-da-0-2-b2.nms...	0	Unlock	Disabled-ANM	gr303	gr303	20	
10.52.30.35_11.1	Cust2	rgvoip-0-d-da-0-2-b2.nms...	1	Unlock	Disabled-ANM	gr303	gr303	47	
10.52.30.35_11.2	CustBG	rgvoip-0-d-da-a-25-2d.nm...	0	Unlock	Disabled-ANM	gr303	gr303	59	
10.52.30.35_11.2	CustBG	rgvoip-0-d-da-a-25-2d.nm...	1	Unlock	Disabled-ANM	gr303	gr303	60	
10.52.30.35_11.2	CustBG	rgvoip-0-d-da-a-25-2d.nm...	2	Unlock	Disabled-ANM	gr303	gr303	61	
10.52.30.35_11.2	CustBG	rgvoip-0-d-da-a-25-2d.nm...	3	Unlock	Disabled-ANM	gr303	gr303	62	
10.52.30.35_11.2	CustBG	rgvoip-0-d-da-a-25-2d.nm...	4	Unlock	Disabled-ANM	gr303	gr303	63	
10.52.30.35_11.2	CustBG	rgvoip-0-d-da-a-25-2d.nm...	5	Unlock	Disabled-ANM	gr303	gr303	64	
10.52.30.35_11.2	CustBG	rgvoip-0-d-da-a-25-2d.nm...	6	Unlock	Disabled-ANM	gr303	gr303	65	
10.52.30.35_11.2	CustBG	rgvoip-0-d-da-a-25-2d.nm...	7	Unlock	Disabled-ANM	gr303	gr303	66	
10.52.30.36_2	sdrADSL8	192.168.1.22	0	Unlock	Disabled-BOTH	gr303	abc	900	failure, failure, failure
10.52.30.36_2	sdrADSL23	192.168.1.22	11	Unlock	Disabled-BOTH	gr303	abc	911	failure, failure, failure
10.52.30.36_2	sdrVDSL8	192.168.1.22	12	Unlock	Disabled-BOTH	gr303	abc	912	failure, failure, failure
10.52.30.36_2	sdrVDSL9	192.168.1.22	13	Unlock	Disabled-BOTH	gr303	abc	913	failure, failure, failure
10.52.30.36_2	sdrVDSL11	192.168.1.22	15	Unlock	Disabled-BOTH	gr303	abc	915	failure, failure, failure
10.52.30.36_2	sdrVDSL12	192.168.1.22	16	Unlock	Disabled-BOTH	gr303	abc	916	failure, failure, failure
10.52.30.36_2	sdrVDSL13	192.168.1.22	17	Unlock	Disabled-BOTH	gr303	abc	917	failure, failure, failure
10.52.30.36_2	sdrVDSL14	192.168.1.22	18	Unlock	Disabled-BOTH	gr303	abc	918	failure, failure, failure
10.52.30.36_2	sdrVDSL15	192.168.1.22	19	Unlock	Disabled-BOTH	gr303	abc	919	failure, failure, failure
10.52.30.36_2	sdrADSL22	192.168.1.22	1	Unlock	Disabled-BOTH	gr303	abc	910	failure, failure, failure
10.52.30.36_2	sdrTestUpgradedPO...	192.168.1.22	2	Unlock	Disabled-BOTH	gr303	abc	506	failure, failure, failure
10.52.30.36_2	sdrADSL11	192.168.1.22	3	Unlock	Disabled-BOTH	gr303	abc	903	failure, failure, failure
10.52.30.36_2	sdrADSL12	192.168.1.22	4	Unlock	Disabled-BOTH	gr303	abc	904	failure, failure, failure
10.52.30.36_2	sdrADSL13	192.168.1.22	5	Unlock	Disabled-BOTH	gr303	abc	905	failure, failure, failure

FIGURE 15-6 GenBand Line Report

15.3 Dual End Line Testing (DELT)

DELT provides information about the quality of the link between the ADSL card and the modem by collecting upstream and downstream values for attainable rate, line attenuation, signal attenuation, signal-to-noise margin, power spectrum density, and aggregate transmitted power. DELT diagnostics are conducted over a low bit rate channel between the iMAP and the CPE and can therefore be executed in extremely degraded cases where the ADSL link cannot train up.

The data collected is based on recommendations of ITU G.997.1 section 7.5.

In addition to line-level attributes, DELT tests also collect signaling information on a sub-carrier basis. For ADSL, there are 512 sub-carriers per line. The sub-carrier data can be graphically displayed to show the characteristics of the line. The graph, in conjunction with signaling templates, can reveal the source or sources of line interference.

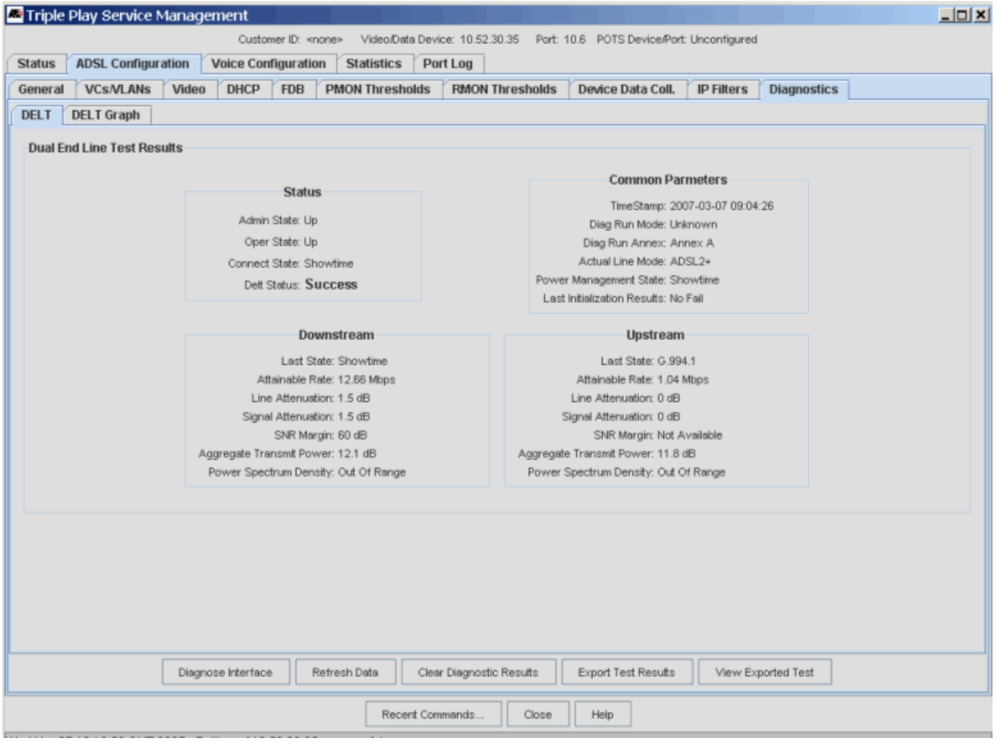
For provisioning, note the following:

- This feature works with the xDSL family (ADSL24A, ADSL24B, ADSL48A, ADSL48B, ADSL24SA, VDSL, PAC24A, ADSL24AE) of cards.
- DELT results are only available if the service module and modem are configured to support one of the ADSL2 modes.
- Not all ADSL2 and ADSL2+ modems support DELT. Running DELT diagnostics on a modem that is not DELT capable will result in a DELT test failure.Since DELT is relatively new capability, inter operability issues exist with some CPE devices. These issues can cause DELT diagnostics to fail, or in some cases, cause DELT to report incorrect results. Allied Telesis will publish a list of CPE (hardware and software versions) that have been verified for proper DELT operation.

Note: The ability for the iMAP to run DELT is from release 9.0, while the NMS DELT feature is for NMS release 10.0. Therefore, this NMS feature can be run on an iMAP running a 9.0 load, although there are some additional DELT feature for iMAP 10.0.

15.3.1 Accessing DELT

From the Port Management application select an active ADSL port one of the supported card types. Select the **ADSL Configuration** tab, then the **Diagnostics** tab. If the tab is not present then the port does not support DELT. Then select the **DELT** tab, as shown in the following figure. If there is existing data from a previous DELT the fields are populated and the **DELT Graph** tab will be active. If there was no previous DELT the **DELT Graph** tab will be inactive and grayed out.



Customer ID: <none> Video/Data Device: 10.52.30.35 Port: 10.6 POTS Device/Port: Unconfigured

Dual End Line Test Results

Status

Admin State: Up
Oper State: Up
Connect State: Showtime
Delt Status: Success

Common Parmeters

TimeStamp: 2007-03-07 09:04:26
Diag Run Mode: Unknown
Diag Run Annex: Annex A
Actual Line Mode: ADSL2+
Power Management State: Showtime
Last Initialization Results: No Fail

Downstream

Last State: Showtime
Attainable Rate: 12.66 Mbps
Line Attenuation: 1.5 dB
Signal Attenuation: 1.5 dB
SNR Margin: 60 dB
Aggregate Transmit Power: 12.1 dB
Power Spectrum Density: Out Of Range

Upstream

Last State: G.994.1
Attainable Rate: 1.04 Mbps
Line Attenuation: 0 dB
Signal Attenuation: 0 dB
SNR Margin: Not Available
Aggregate Transmit Power: 11.8 dB
Power Spectrum Density: Out Of Range

FIGURE 15-7 DELT Testing Tab

15.3.2 Initiate a DELT Diagnostic

Clicking the **Diagnose Interface** button will initiate a DELT. A confirmation dialog box appears indicating that service may be disrupted, if confirmed the ATI activity dialog appears until the test starts. While running, all the buttons are disabled except for **View Exported Test**. The "DELT Status" field indicates "Running" or "In Progress" while the test is running. When successfully completed the basic result values will populate the fields, the **DELT Graph** tab will be activated, and all the buttons will be enabled.

15.3.3 Retrieve DELT Results

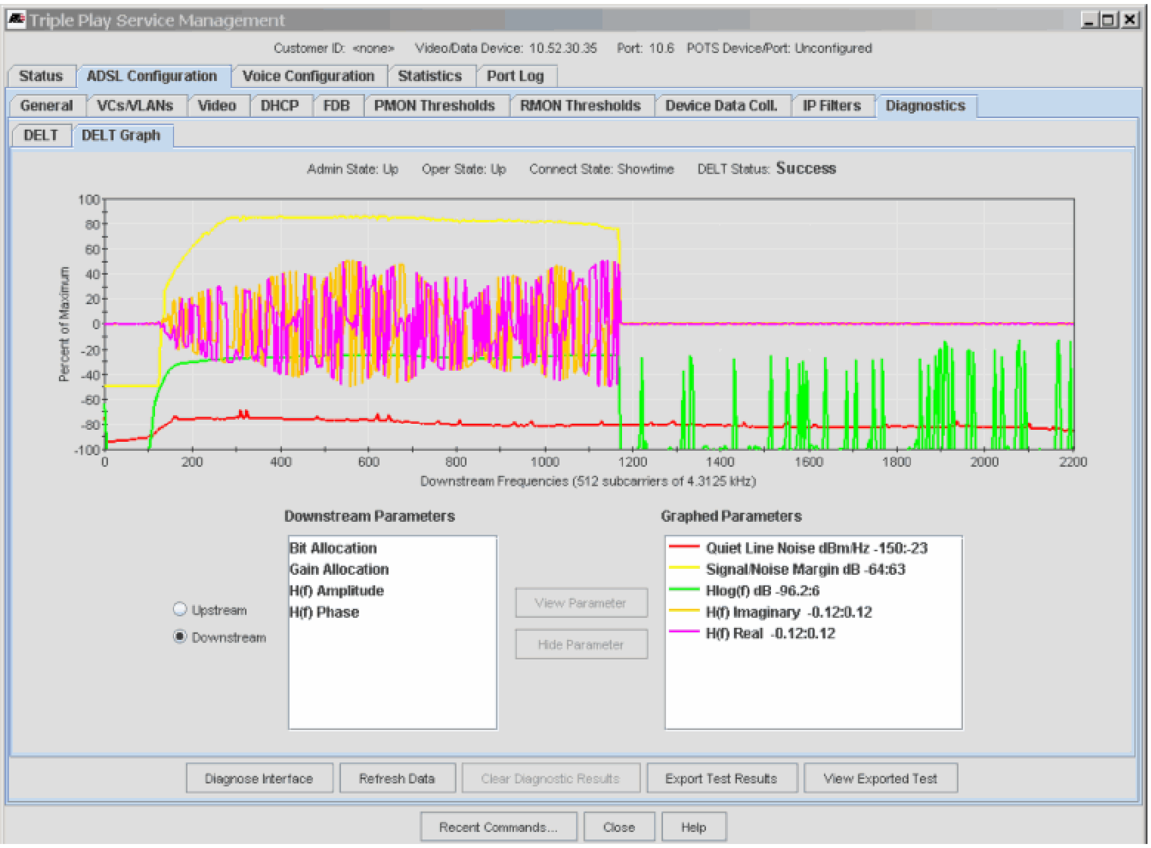
DELT results are automatically retrieved when the **DELT** tab is selected, and after a successful DELT test. Clicking the **Refresh Data** button will re-retrieve this data, along with the current mode of the port. If the port Mode is unknown, due to the port retraining after the last test, this will also update that field.

15.3.4 Graph DELT Result

When DELT results exist the **DELT Graph** tab is activated. Selecting it will display the following screen. Initially all parameters are in the left window and none are graphed. Selecting one or more and clicking the **View Parameter** button will move it into the right "Graphed Parameters" list and draw a graph of its data. The color of the line used is shown next to the graphed parameter name. (To remove a parameter, select one or more in the "Graphed Parameters" list and click the **Remove Parameter** button.

The same parameters are available for both upstream and downstream directions, though different numbers of sub carriers are available based on the actual mode of the port. Selecting a different direction will clear the graph, move all parameters back the available list, and switch the data to the selected direction.

Clicking the **Refresh Data** button will recollect the data from the iMAP just as it does on the **DELT** tab. This will only have an effect if the mode of the port changes or if a new DELT was run, or the results cleared, outside of the NMS.



Customer ID: <none> Video/Data Device: 10.52.30.35 Port: 10.6 POTS Device/Port: Unconfigured

Admin State: Up Oper State: Up Connect State: Showtime DELT Status: Success

Downstream Parameters:

Bit Allocation
Gain Allocation
H(f) Amplitude
H(f) Phase

Graphed Parameters:

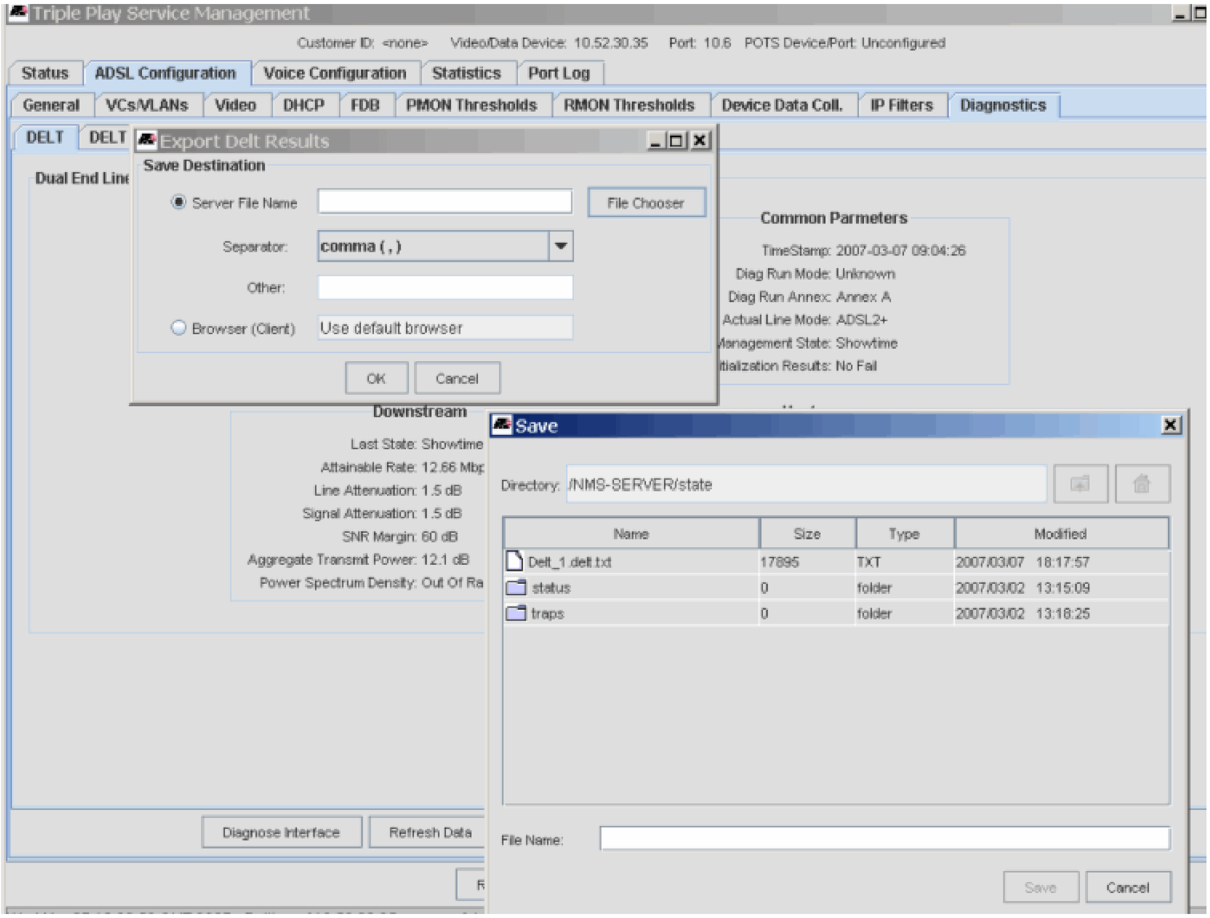
🟥 Quiet Line Noise dBm/Hz -150:-23
🟨 Signal/Noise Margin dB -64:63
🟩 Hlog(f) dB -96.2:6
🟧 H(f) Imaginary -0.12:0.12
🟪 H(f) Real -0.12:0.12

FIGURE 15-8 Graph of DELT Parameter Results

15.3.5 Export DELT Results to a File

Clicking the **Export Test Results** button displays an export dialog similar to the one used for exporting other data from the NMS. Data is stored on the NMS server. If the **File Chooser** button is clicked, you can navigate to a directory on the server and select an existing file or create a new one. When the **OK** button on the export dialog is clicked the data is stored on the NMS server in the indicated file.

Note: *If the test is from an iMAP running 9.x, the timestamp is set to the time the results are saved. When the test is viewed, this time is shown as the timestamp value.*



Customer ID: <none> Video/Data Device: 10.52.30.35 Port: 10.6 POTS Device/Port: Unconfigured

● Server File Name

Separator: comma (,)

Other:

○ Browser (Client) Use default browser

TimeStamp: 2007-03-07 09:04:26
Diag Run Mode: Unknown
Diag Run Annex: Annex A
Actual Line Mode: ADSL2+
lanagement State: Showtime
itialization Results: No Fail

Last State: Showtime
Attainable Rate: 12.66 Mbp
Line Attenuation: 1.5 dB
Signal Attenuation: 1.5 dB
SNR Margin: 60 dB
Aggregate Transmit Power: 12.1 dB
Power Spectrum Density: Out Of Ra

Directory: /NMS-SERVER/state

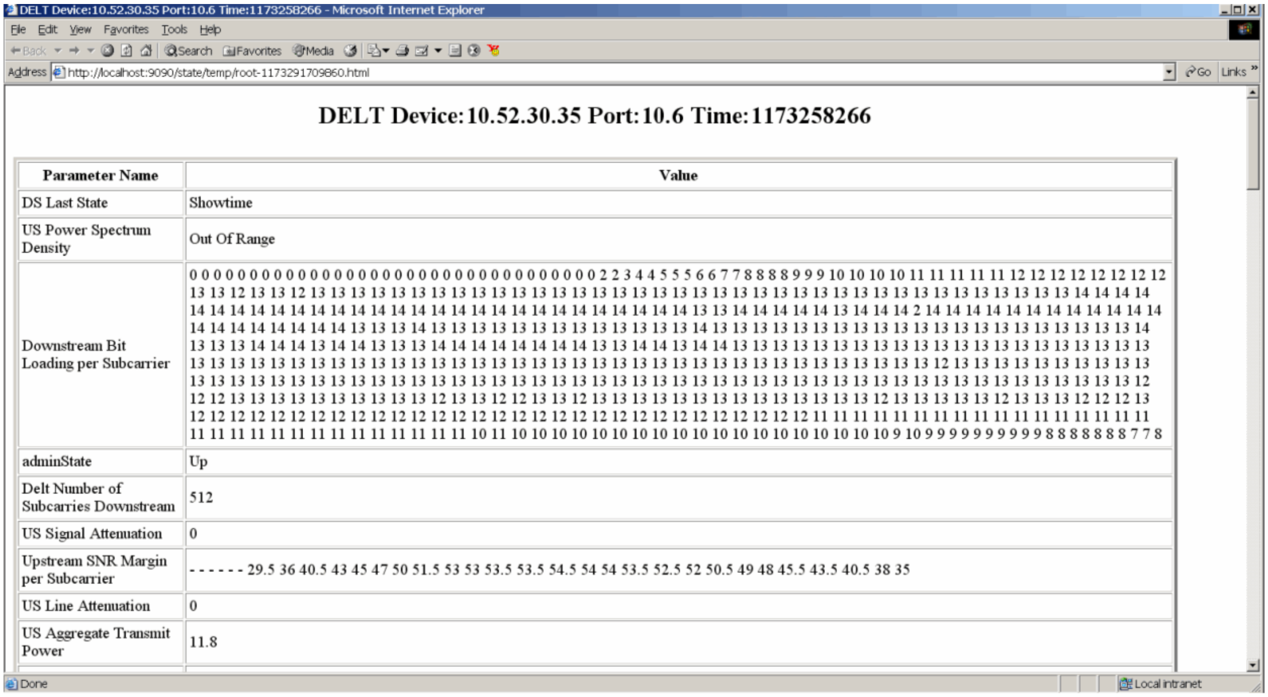
Name	Size	Type	Modified
Delt_1.delt.txt	17895	TXT	2007/03/07 18:17:57
status	0	folder	2007/03/02 13:15:09
traps	0	folder	2007/03/02 13:18:25

File Name:

FIGURE 15-9 Exporting DELT Results to a File

15.3.6 Export DELT Results to Web Page

As with other export operations, the data can optionally be exported to an HTML page and viewed with a browser. The page can then be saved using the browser.


DELT Device:10.52.30.35 Port:10.6 Time:1173258266 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://localhost:9090/state/temp/root-1173291709860.html
Go Links
Done
Local intranet

DELT Device:10.52.30.35 Port:10.6 Time:1173258266

Parameter Name	Value
DS Last State	Showtime
US Power Spectrum Density	Out Of Range

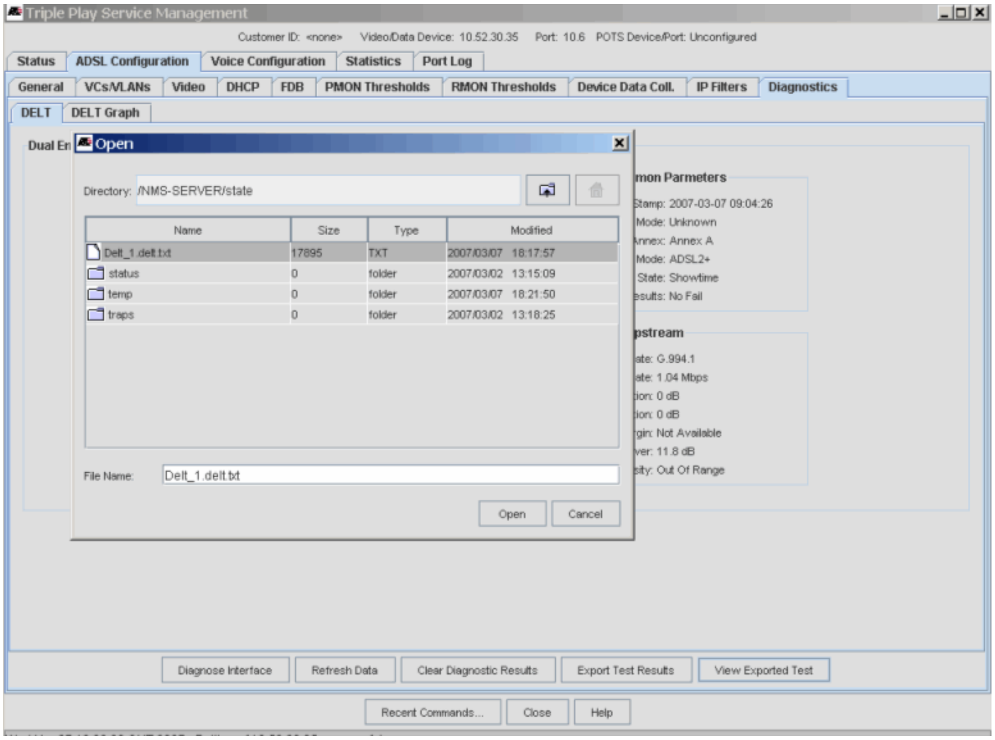
Downstream Bit Loading per Subcarrier	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 2 2 3 4 4 5 5 5 6 6 7 7 8 8 8 8 9 9 9 10 10 10 10 11 11 11 11 11 12 12 12 12 12 12 12 12
	13 13 12 13 13 12 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 14 14 14 14
	14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 13 13 14 14 14 14 14 13 14 14 14 2 14 14 14 14 14 14 14 14 14 14 14 14
	14 14 14 14 14 14 14 14 13 13 13 14 13 13 13 13 13 13 13 13 13 13 13 13 13 14 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 14
	13 13 13 14 14 14 13 14 14 13 13 13 14 14 14 14 14 14 14 14 13 13 14 14 13 14 14 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13
	13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 12 13 13 13 13 13 13 13 13 13 13
	13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 13 12
	12 12 13 13 13 13 13 13 13 13 13 13 12 13 13 12 12 13 13 12 13 13 13 13 13 13 13 13 13 13 13 13 13 13 12 13 13 13 13 13 12 13 13 13 12 12 12 13
	12 12 12 12 12 12 12 12 12 12 12 12 12 12 12 12 12 12 12 12 12 12 12 12 12 12 12 12 12 12 12 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11
	11 11 11 11 11 11 11 11 11 11 11 11 11 11 10 11 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 9 10 9 9 9 9 9 9 9 9 9 9 8 8 8 8 8 8 8 7 7 8

adminState	Up
Delt Number of Subcarries Downstream	512
US Signal Attenuation	0
Upstream SNR Margin per Subcarrier	- - - - - - 29.5 36 40.5 43 45 47 50 51.5 53 53 53.5 53.5 54.5 54 54 53.5 52.5 52 50.5 49 48 45.5 43.5 40.5 38 35
US Line Attenuation	0
US Aggregate Transmit Power	11.8

FIGURE 15-10 Exporting DELT Results to a Web Page

15.3.7 Viewing Exported DELT Results

DELT results exported to a file can be viewed from using the **View Exported Test** button on the Port Details ADSL diagnostics tab. First a file chooser is displayed to select the file containing the test results.



Customer ID: <none> Video/Data Device: 10.52.30.35 Port: 10.6 POTS Device/Port: Unconfigured

Directory: /NMS-SERVER/state

Name	Size	Type	Modified
Delt_1.delt.txt	17895	TXT	2007/03/07 18:17:57
status	0	folder	2007/03/02 13:15:09
temp	0	folder	2007/03/07 18:21:50
traps	0	folder	2007/03/02 13:18:25

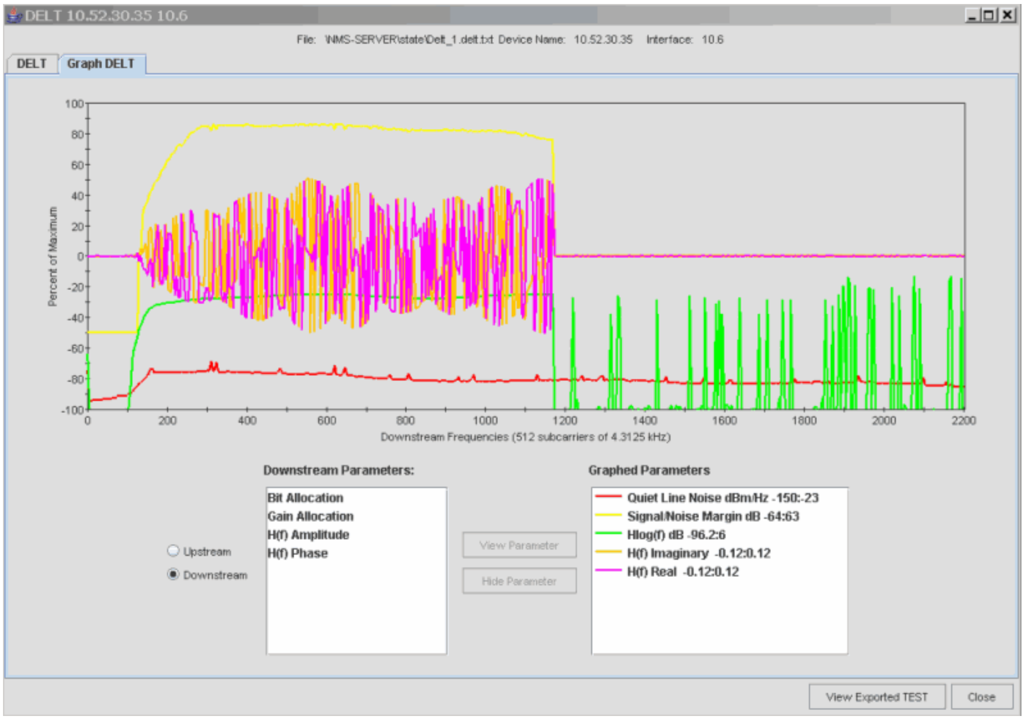
File Name: Delt_1.delt.txt

Stamp: 2007-03-07 09:04:26
Mode: Unknown
nnex: Annex A
Mode: ADSL2+
State: Showtime
esults: No Fail

ate: G.994.1
ate: 1.04 Mbps
ion: 0 dB
ion: 0 dB
gin: Not Available
ver: 11.8 dB
sity: Out Of Range

FIGURE 15-11 View Exported DELT Results

After a file is selected the test result viewer is displayed. The viewer window also has a **View Exported Test** button so that additional tests can be displayed and compared. A maximum of eight (8) tests can viewed simultaneously from a single client, in addition to the port details window. Refer to the following figure.



File: \NMS-SERVER\state\Delt_1.delt.txt Device Name: 10.52.30.35 Interface: 10.6

Downstream Parameters:

Bit Allocation
Gain Allocation
H(f) Amplitude
H(f) Phase

Graphed Parameters

🟥 Quiet Line Noise dBm/Hz -150:-23
🟨 Signal/Noise Margin dB -64:63
🟩 Hlog(f) dB -96.2:6
🟧 H(f) Imaginary -0.12:0.12
🟪 H(f) Real -0.12:0.12

FIGURE 15-12 View Graph Results

15.3.8 Graphed Parameters

- Subcarriers - The same values are available for both upstream and downstream directions. Depending on the type of port and actual mode of operation different subcarrier counts are used. The following table describes the possible values

TABLE 15-3 Values for Subcarriers

Card Types	Actual Standard	Actual Annex	Upstream Carriers	Downstream Carriers
VDSL24A, VDSL24B			512	512
ADSL24A/B, ADSL24AE ADSL48A, ADSL48B,	ADSL2, ADSL2M	ANNEXB, ANNEXM	64	256
		others	32	256
	ADSL2+ ADSL2+M	ANNEXB, ANNEXM	64	512
			32	512

- Bit Loading - Bits allocated per sub channel. Range is 0 to 15.
- Gain - Range is 0 - 4093/512.
- Quiet Line Noise - Noise on quite line. Range is -150 to -23 db/MHz.
- Signal/Noise Margin - The signal-to-noise ratio margin per band is the maximum increase in dB of the noise power received at the xTU-R, such that the BER requirements are met for all bearer channels. The range is from -64 dB to +63 dB with 0.1 dB steps.
- Hlog(f) - The log of the characteristic function
- H(f) Imaginary - The imaginary component of the characteristic function.
- H(f) Real - The real component of the characteristic function.
- H(f) Amplitude - The amplitude of the characteristic function. This is computed from the real and imaginary components. *Amp = sqrt(r*r + i*i)* where r is the real component and i the imaginary component.
- H(f) Phase - The phase of the characteristic function. This is computed from the real and imaginary components. *Phase = atan(i/r)* where r is the real component and i the imaginary component.

15.4 Single-End Line Testing (SELT)

15.4.1 Overview of SELT

SELT is a method for testing a DSL loop that is **not** terminated at the CPE. These tests provide for the loop information on the length, the presence of open or short circuits, and estimates of pre-service capacity.

SELT testing is usually done in the following scenarios:

- Pre-CPE Installation - The loop exists, but not at the CPE. SELT can test the line for physical bridge and loop taps.
- Pre-CPE Activation - SELT can characterize the loop and measure loop noise. The information can be used to determine maximum rates.
- Post Activation - If there is a problem, the characterization of the loop can be compared to the results of the pre-CPE activation to see if there are any changes.

This feature works with the xDSL family (ADSL24A, ADSL24B, ADSL24SA, ADSL24AE, ADSL48A, and ADSL48B) of cards. (VDSL cards will be supported in a future release.)

SELT sessions are limited to a single session at a time due to the amount of time (up to four minutes) each test can take to complete and the resources needed to execute the test.

For accurate results, loops up to 9000 feet can be tested. Using the FULL options allows loops up to 12,000 feet can be tested. Limits are as follows:

Annex B support is limited to 24 AWG loops. 26 AWG wiring is not supported and will produce erroneous results

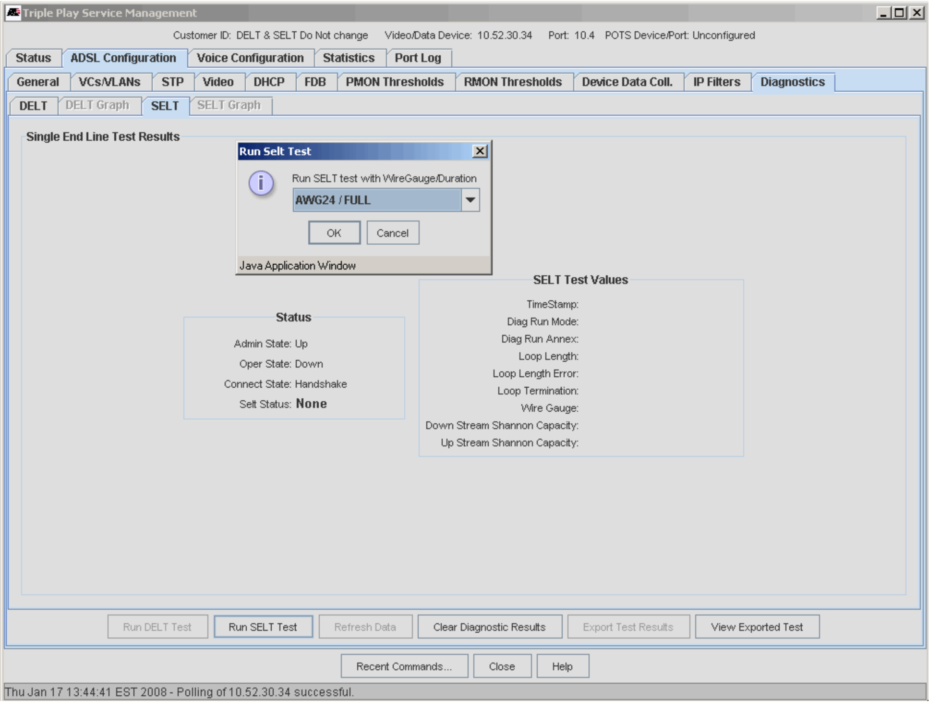
The port/interface to be tested must be in operationally down: UP-DN-Failed. The state life-cycle for the port/interface under test will be: UP-DN-Failed to start the test, UP-DN-In Test for the duration of the test and will be transitioned back to UP-DN-Failed once testing has completed.

Refer to the *Software Reference for iMAP Series Switches* for details on SELT testing.

15.4.2 Accessing SELT

From the Port Management application select an active ADSL port one of the supported card types. Select the **ADSL Configuration** tab, then the **Diagnostics** tab. If the tab is not present then the port does not support SELT. Then select the **SELT** tab, as shown in the following figure. If there is existing data from a previous SELT the fields are populated and the **SELT Graph** tab will be active. If there was no previous SELT the **SELT Graph** tab will be inactive and grayed out.

To run SELT, select the **Run SELT Test** button. A panel appears with the options for the test. Refer to the following figure.



Triple Play Service Management

Customer ID: DELT & SELT Do Not change Video/Data Device: 10.52.30.34 Port: 10.4 POTS Device/Port: Unconfigured

Run Selt Test

Run SELT test with WireGauge/Duration

AWG24 / FULL

Java Application Window

Status

Admin State: Up

Oper State: Down

Connect State: Handshake

Selt Status: None

SELT Test Values

TimeStamp:

Diag Run Mode:

Diag Run Annex:

Loop Length:

Loop Length Error:

Loop Termination:

Wire Gauge:

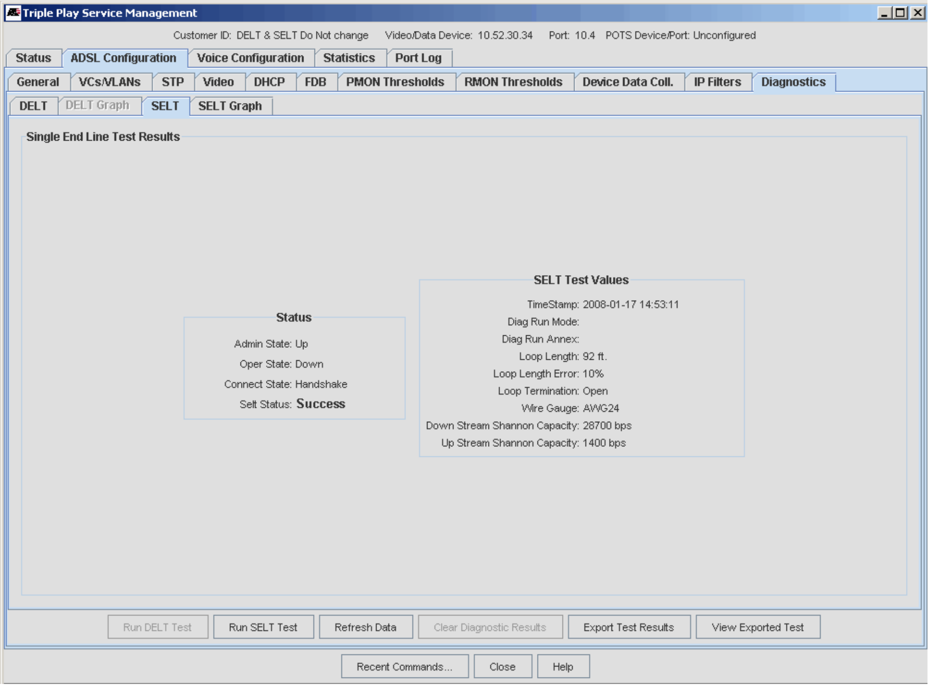
Down Stream Shannon Capacity:

Up Stream Shannon Capacity:

Thu Jan 17 13:44:41 EST 2008 - Polling of 10.52.30.34 successful.

FIGURE 15-13 Running the SELT Test

Select OK, and the test will begin. As it goes through testing, the state will change, until the test is complete and with a status of Success. Refer to the following figure.



Customer ID: DELT & SELT Do Not change Video/Data Device: 10.52.30.34 Port: 10.4 POTS Device/Port: Unconfigured

Status

Admin State: Up
Oper State: Down
Connect State: Handshake
Selt Status: **Success**

SELT Test Values

TimeStamp: 2008-01-17 14:53:11
Diag Run Mode:
Diag Run Annex:
Loop Length: 92 ft.
Loop Length Error: 10%
Loop Termination: Open
Wire Gauge: AWG24
Down Stream Shannon Capacity: 28700 bps
Up Stream Shannon Capacity: 1400 bps

FIGURE 15-14 SELT Test Complete

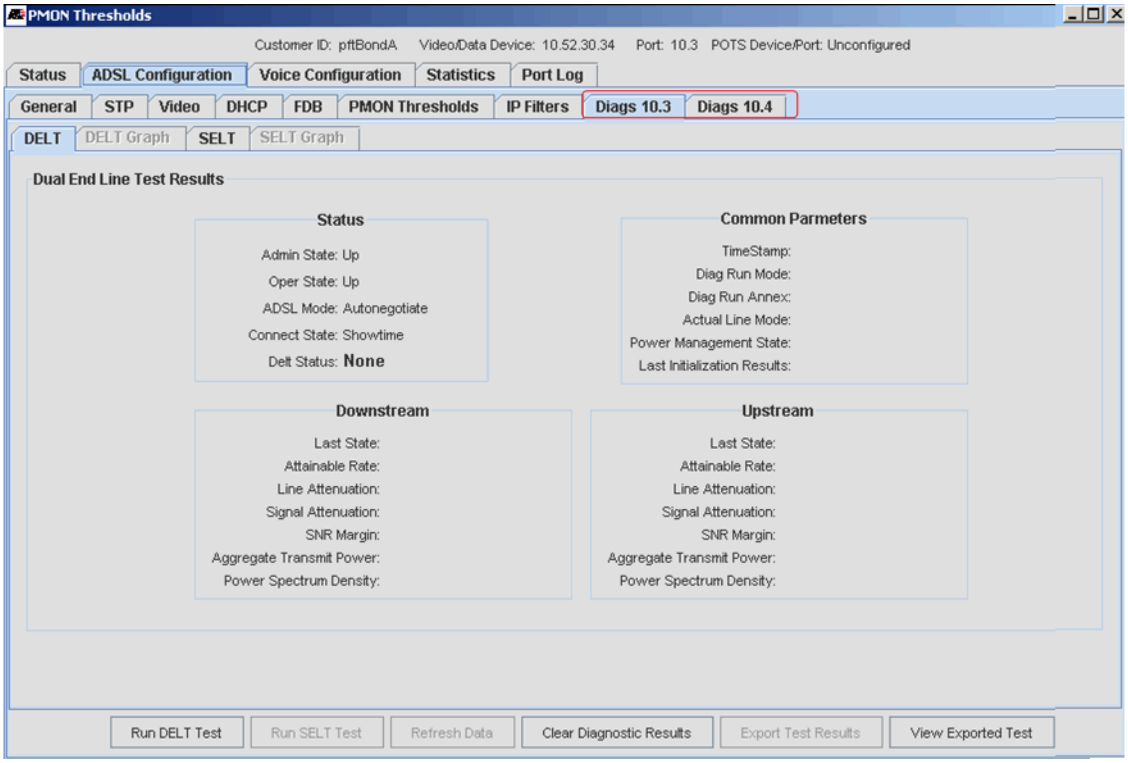
Once the test is complete, the user can view the results on a browser or save the test results for later analysis. The interface to review test results is similar to those used for DELT and is described in "Dual End Line Testing (DELT)" on page 501.

15.5 Diagnostics for ATMBOND

DELT (Dual End Line Test) and SELT (Single End Line Test) can be run on each ADSL port when they are in the appropriate state:

- For DELT that is Up/Up/Showtime
- For SELT Up/Down

Note: These tests may not actually work with the particular modems being used



Customer ID: pftBondA Video/Data Device: 10.52.30.34 Port: 10.3 POTS Device/Port: Unconfigured

Dual End Line Test Results

Status

Admin State: Up
Oper State: Up
ADSL Mode: Autonegotiate
Connect State: Showtime
Delt Status: **None**

Common Parmeters

TimeStamp:
Diag Run Mode:
Diag Run Annex:
Actual Line Mode:
Power Management State:
Last Initialization Results:

Downstream

Last State:
Attainable Rate:
Line Attenuation:
Signal Attenuation:
SNR Margin:
Aggregate Transmit Power:
Power Spectrum Density:

Upstream

Last State:
Attainable Rate:
Line Attenuation:
Signal Attenuation:
SNR Margin:
Aggregate Transmit Power:
Power Spectrum Density:

FIGURE 15-15 ATMBOND Diags

15.6 Support of CWMP with TR-069 Devices

Caution: Caution: Due to inter operability problems, do NOT use the TR-069 CPE WAN Management Protocol (CWMP) to manage Comtrend 5631 CPE. Otherwise, service may be interrupted. Instead, use the Comtrend web GUI for configuration and management. Contact your ATI representative for details.

15.6.1 Overview

Support of CWMP with TR-069 provides:

- The CPE Wan Management Protocol (CWMP) TR-069 framework is supported.
- Basic support for the Comtrend 5631 CPE device.

This Comtrend device supports bonded ports where multiple ADSL lines are combined (bonded) together and connected to one CPE device to allow higher throughput rates for the individual customer using the CPE. This feature is expected to be used to configure the iMAP ports where the Comtrend CPE is connected. Refer to the following figure, keeping in mind the following provisioning guidelines:

- The G.bond feature requires support for up to two (2) ADSL bonded ports.
- Unlike the SHDSL wire-pair bonding implementation which requires the bonded ports to be adjacent, G.bond allows for any two ports to bond together as long as they exist on the **same card**.

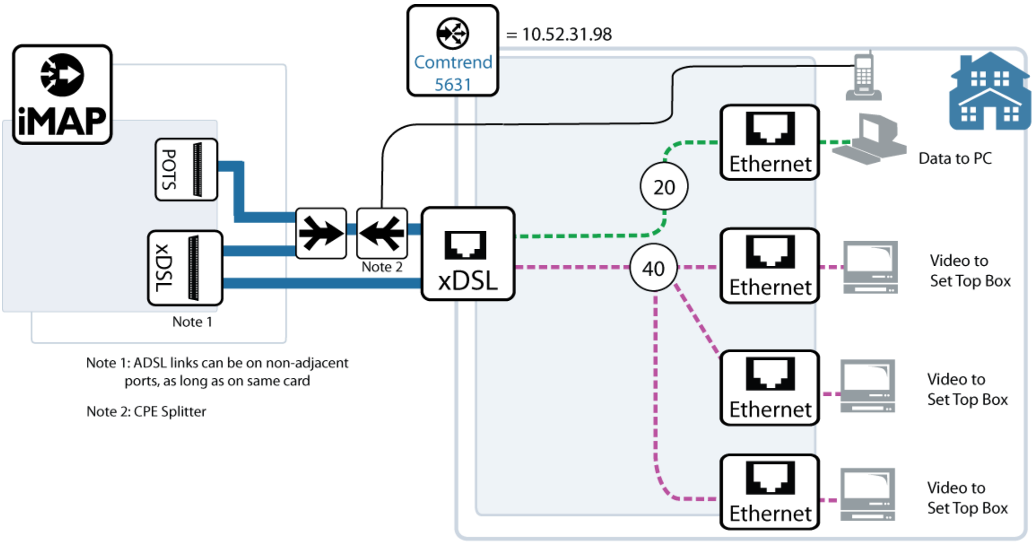


FIGURE 15-16 Comtrend Configuration (Bonded ADSL)

15.6.2 Basic Functions

The following functions are provided:

- Provisioning of the Comtrend device using the NMS

  Video and internet services can be provisioned using the NMS Triple-Play GUIs, using TR-069. Existing Profiles can be used with the Comtrend CPE as with other iMG/RGs.

- Backup and Restore

  The Comtrend configuration files can be backed up and restored as with other CPE devices.

- Display and modify device information using the Multi-device Table Interface (MDTI) applications

  The Comtrend CPE is added.

Note: *Although there is now support for provisioning the Comtrend using the NMS, there are limitations, since some components supported by the NMS are not yet implemented in the Comtrend CPE, and the Comtrend CPE does not fully support TR-069 and related specifications. This is explained through the rest of this Section.*

Support for this device includes:

- Viewing Managed Object Properties
- Provisioning a new customer/CPE
- Initiate device rediscovery
- De-provision customer/CPE
- Remove Profile association
- Monitoring operations (Alarms/Events)
- Providing access to provision the device through
  - a browser to access the device web server
  - telnet to allow CLI

The following figure shows the menu options available (right-click device in Inventory)

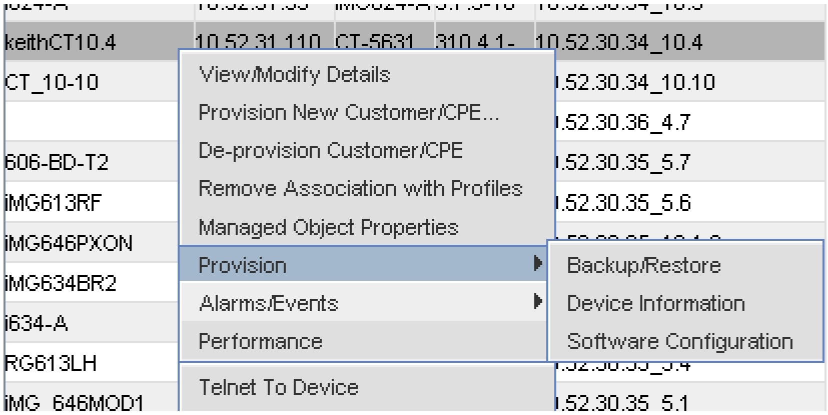


FIGURE 15-17 Menu Items Available for Comtrend (Provision added in SP5)

15.6.3 Feature Limitations

Although provisioning the Comtrend uses the same GUI panels as other CPE devices, there are limitations because certain features supported on the NMS are not supported on the Comtrend CPE, and this affects the provisioning process and tools that are used, detailed in "Provisioning Flow" on page 512.

- The upstream port cannot be determined, and so provisioning is done using the CPE MAC address. This is similar to provisioning an iMG without an iMAP. Refer to "Provisioning the iMG (no iMAP or AW+)" on page 873.
- An Auto-Configuration Server (ACS) URL must be configured in the CPE for using TR-069 for communicating with the ACS (the NMS). The current release of the Comtrend CPE is not able to use DHCP to configure the ACS URL, and so for SP5 the **Comtrend Boot Configurator** must be used. Refer to "Comtrend Boot Configurator" on page 513.
- Customer ID (SysContact on CPE) is limited to 15 characters. If more than 15 characters are used when provisioning a triple play customer, the iMAP ADSL bond port will use the entire string, but the Comtrend CPE SysContact will be truncated to 15 characters, resulting in more complex customer management.
- Derived voice service is not supported unless the VoIP phone is connected directly an Ethernet port and the CPE can provide a bridged Ethernet connection. When provisioned this way, the VoIP features will not be managed by NMS.
- The only supported internet service is Bridged.
- For Video, only IGMP snooping enabled is supported on the CPE.
- Only a subset of wireless features can be configured using the NMS.
- The Compare Profile feature is not supported.
- The MDTI feature software configuration is not supported, since the software file uses a different format.
- The NMS must use the configuration file to make most of the changes to the CPE and then sends it back to the CPE using TFTP or CWMP (the default is TFTP). Therefore, when any changes are made (using the Service Management panels), the configuration file is updated and the CPE must reboot for the changes to take effect. During this reboot services are dropped until the CPE returns to service.

15.6.4 Provisioning Flow

Taking the feature limitations into account, as listed in "Feature Limitations" on page 512, provisioning the Comtrend CPE involves the following concepts:

1. Before a Comtrend CPE device is sent to a customer, it will first need to be connected to a PC (the NMS server) to enable the default device configuration. The provider will run the Comtrend Boot Configurator Tool and upload the default boot configuration to the CPE which will add the management VLAN and TR-069 information so that it can be managed using TR-069. It also includes the Inform interval.

2. Existing iMG/RG profiles (General, Internet and Video) can be used, but not all values in these profiles will apply. Non-applicable parameters will be skipped when the profile is deployed or used to provision the CPE.
3. When provisioning the Triple Play form, the CPE MAC address is required because it cannot be correctly determined automatically and mapped with device port when needed.

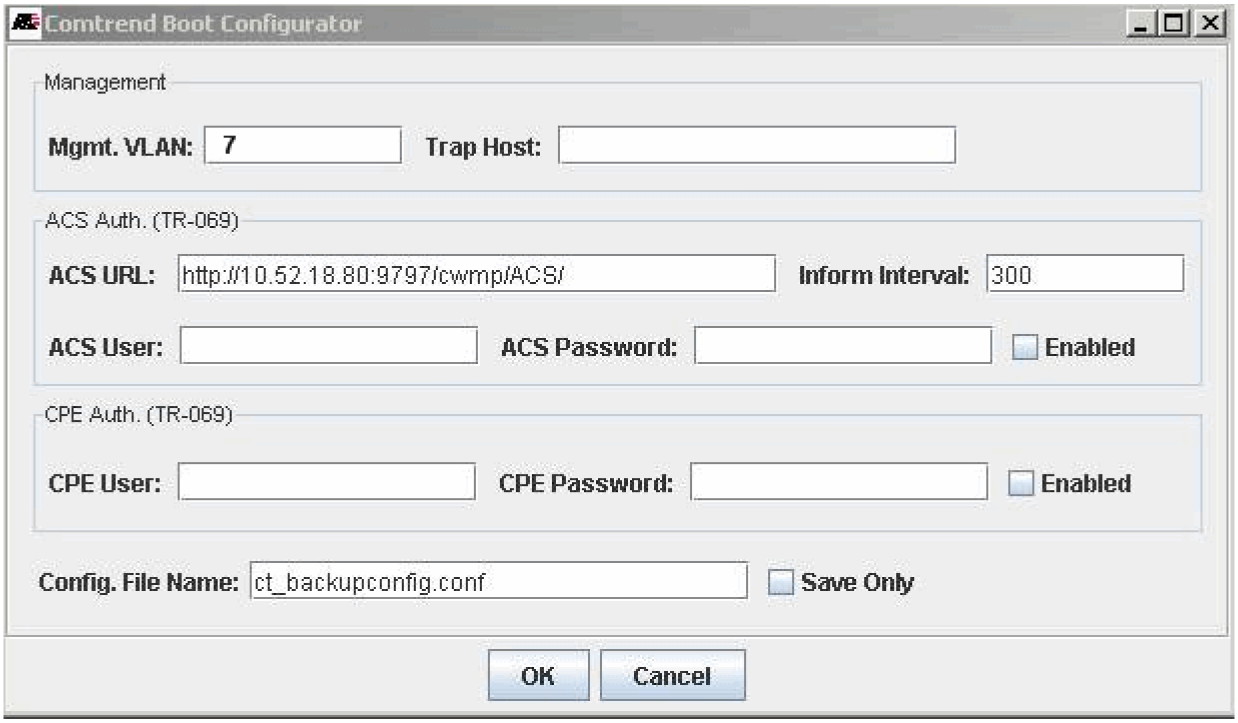
Note: With the Comtrend provisioned with a specific MAC address, it cannot simply be swapped with another unit when performing provisioning or maintenance and having the NMS automatically provision the new unit. The old unit would need to be deprovisioned, then the provisioning process would need to start again.

4. The Comtrend CPE only allows one CLI login session at a time (for example, if CLI is used to initiate TFTP to the device). Therefore, login to the CPE device will fail if another user is already logged in.

Caution: While an administrator is logged into the CPE, the NMS cannot login, and so some features will not work.

15.6.5 Comtrend Boot Configurator

The Comtrend Boot Configurator is a tool that allows updating the Comtrend CPEs to use management configuration parameters and is similar to the Boot Configurator used for iMG/RGs. The main difference is that since Comtrend CPEs do not support getting the TFTP server address through DHCP, you must use the tool to generate the default configuration and then upload it to the device. The following figure shows a sample Comtrend Boot Configurator panel with values filled in.



Comtrend Boot Configurator

Management

Mgmt. VLAN: 7

Trap Host:

ACS Auth. (TR-069)

ACS URL: http://10.52.18.80:9797/cwmp/ACS/

Inform Interval: 300

ACS User:

ACS Password:

□ Enabled

CPE Auth. (TR-069)

CPE User:

CPE Password:

□ Enabled

Config. File Name: ct_backupconfig.conf

□ Save Only

FIGURE 15-18 Comtrend Boot Configurator

The fields in this form are as follows:

- **Mgmt. VLAN** - The VLAN used for sending and receiving configuration information and downloads to the CPE.
- **Trap Host** - The IP address of the Auto Configuration Server (ACS) - the NMS.
- **ACS URL** - An ACS URL is required to be configured in CPE for using TR-069 for communication with the ACS server (NMS). The ACS URL pointing to NMS server should be:

  http://<NMS IP address>:9797/cwmp/ACS/

Note: The port number has changed; in SP3 this was 9090.

- **Inform Interval** - How often (in seconds) the CPE contacts the ACS with identification information. The default is 300 (five minutes).
- **ACS User** and **Password** - The User ID and password to access the ACS server. The CPE uses this to communicate with the ACS.
- **CPE User** and **Password** - User ID and password to access the CPE. The NMS uses this to communicate with the CPE.
- **Config File Name** - The name of the configuration file on the TFTP server that includes the values selected here.
- **Save Only** - If checked, the settings for the configuration file are saved but are not uploaded to the CPE (there is no physical connection between the ACS and CPE).

15.6.6 Staging - Summary

As explained in "Provisioning Flow" on page 512, there is a staging procedure needed for the Comtrend devices so that they may be provisioned. Staging can be accomplished using one of the following two methods summarized below:

- Method 1

  Run the Comtrend Boot Configurator at the NMS server. Check the Save Only checkbox before clicking OK. Then copy the configuration file to a PC connected to a LAN port on the Comtrend. Use the web GUI on the Comtrend to update settings with the configuration file.

- Method 2

  Install and run the NMS server software on a PC connected to a LAN port on the Comtrend. You must run the NMS server software so the TFTP server is running. Run the Comtrend Boot Configurator at this PC. Do not check the Save Only checkbox before clicking OK.

Note: The Comtrend could be connected to the NMS server that is used to manage the network. However, since this would allow access to the network devices, this is not recommended.

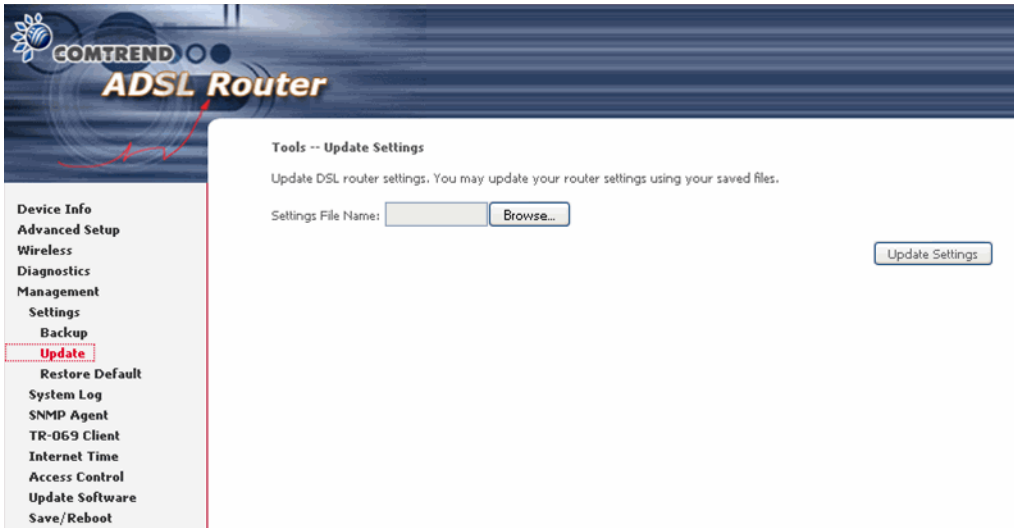
15.6.7 Staging - Method 1

- Prerequisites
  - The Comtrend is set to factory defaults.
  - A PC is connected to a LAN port on the Comtrend device. The PC obtains an IP address automatically from the Comtrend.

1. At the NMS server, access the Comtrend Boot Configurator by going to `<NMS_Home>/bin` and double-clicking on **AT_CTBootConfigurator.**
2. On the Comtrend Boot Configurator Form (Figure 5-204), the only fields that must be filled in are:
   - Mgmt. VLAN
   - ACS URL

Note: For a description of these and other fields, refer to Figure 15.6.5.

3. Check the **Save Only** checkbox. Click on **OK**.
4. Go to `<NMS_Home>/tftp/Comtrend` and locate the configuration file, for example `ct_backupconfig.conf`. Copy the configuration file to a PC connected to a LAN port of the Comtrend.
5. At the PC connected to the Comtrend, open a web browser and go to http://192.168.1.1/ to access the Comtrend web GUI. Log in with User Name root, and Password 12345. In the GUI sidebar, select *Management* > *Settings* > *Update*. The Tools - Update Settings page opens as shown in Figure 15-19.



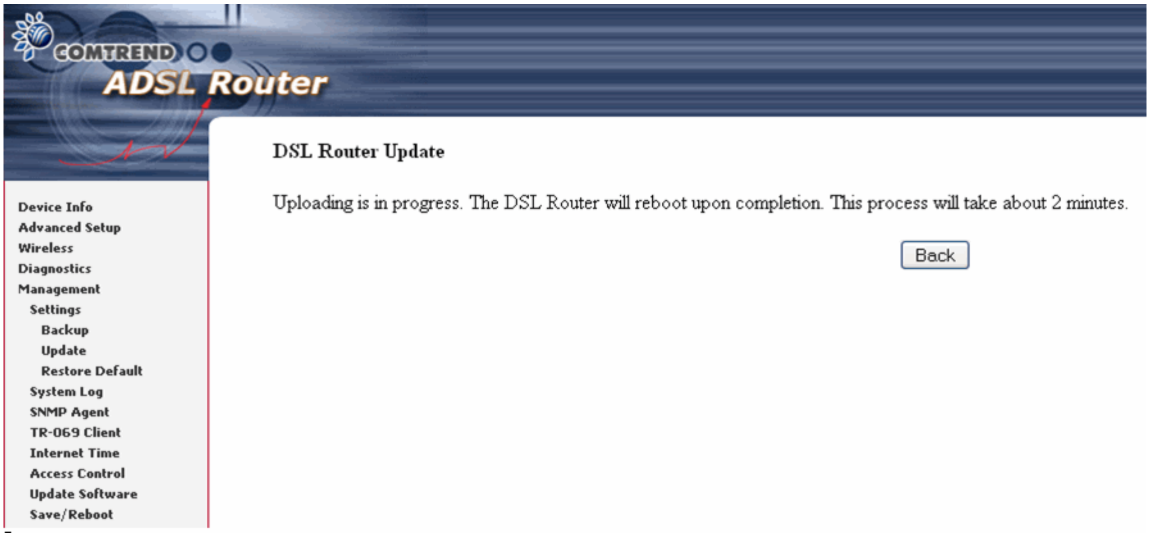
Tools -- Update Settings

Update DSL router settings. You may update your router settings using your saved files.

Settings File Name:

FIGURE 15-19 Comtrend Tools - Update Settings

6. In the Settings File Name field, enter or browse to the configuration file copied in step 4. Click **Update Settings**. The Comtrend reboots (Figure 15-20). The Comtrend is now ready to be deployed



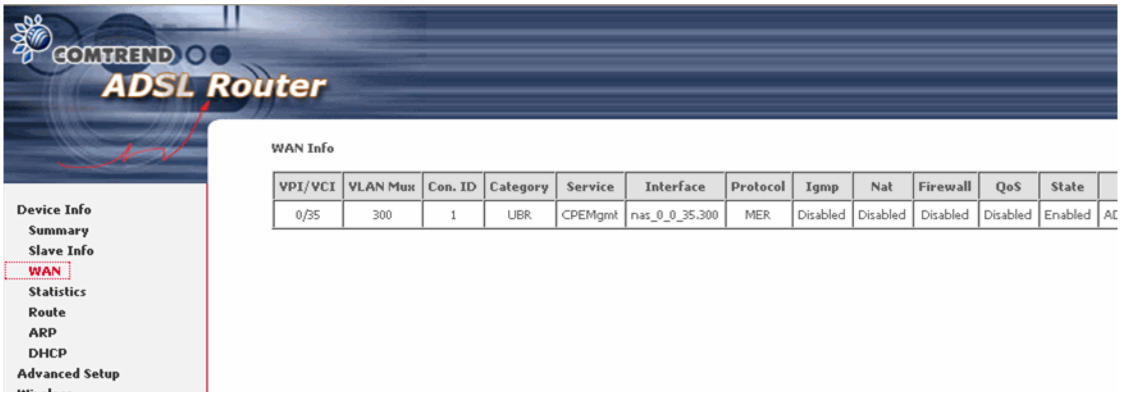
DSL Router Update

Uploading is in progress. The DSL Router will reboot upon completion. This process will take about 2 minutes.

FIGURE 15-20 Updating Comtrend with Configuration File

Note: The following steps are optional.

7. After the Comtrend has rebooted, to verify settings, select *Device Info* > *WAN*. The WAN Info page should show the CPE Mgmt service provisioned with the VLAN specified in step 2. Refer to Figure 15-21.

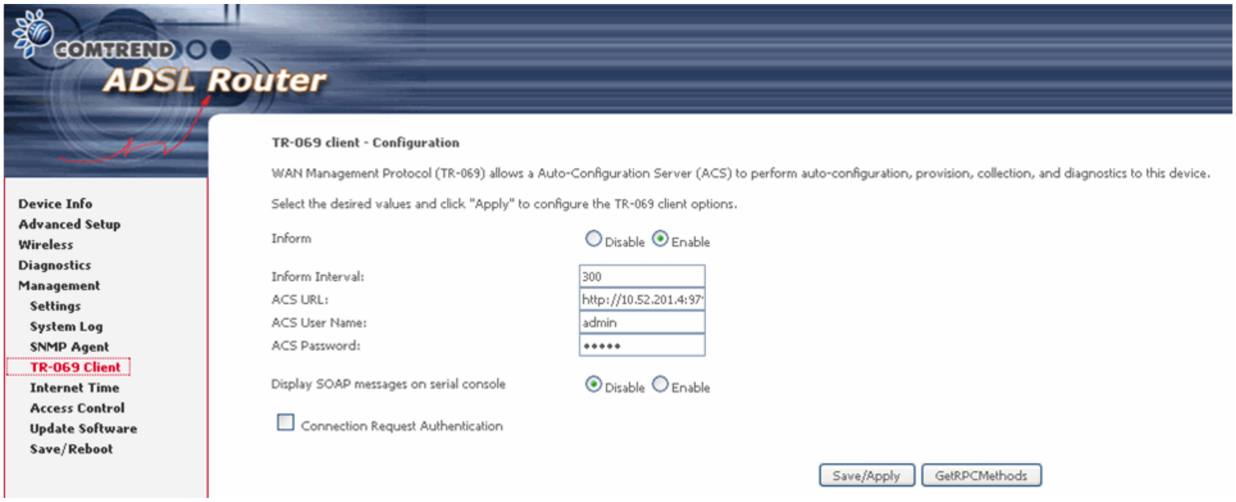


WAN Info

VPI/VCI	VLAN Mux	Con. ID	Category	Service	Interface	Protocol	Igmp	Nat	Firewall	QoS	State	
0/35	300	1	UBR	CPEMgmt	nas_0_0_35.300	MER	Disabled	Disabled	Disabled	Disabled	Enabled	AD

FIGURE 15-21 Comtrend WAN Info

8. Select *Management* > *TR-069 Client*. The TR-069 client - Configuration page should show the ACS URL and other fields set to the values specified in step 2. Refer to Figure 15-22.



TR-069 client - Configuration

WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

Select the desired values and click "Apply" to configure the TR-069 client options.

Inform ○ Disable ● Enable

Inform Interval: 300
ACS URL: http://10.52.201.4:97
ACS User Name: admin
ACS Password: •••••

Display SOAP messages on serial console ● Disable ○ Enable

□ Connection Request Authentication

FIGURE 15-22 Comtrend TR-069 client - Configuration

15.6.8 Staging - Method 2

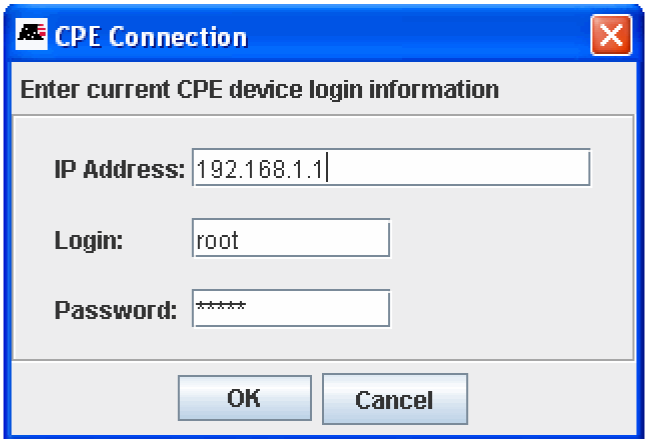
- Prerequisites:
  - The Comtrend is set to factory defaults.
  - A local PC (desktop/laptop, etc.) has been loaded with the NMS release 11.0 SP5 software.
  - The local PC is connected to a LAN port on the Comtrend device. The PC obtains an IP address automatically from the Comtrend.

The specific steps are as follows:

1. Start up the local NMS on the local PC (*Programs->AlliedView NMS->Start NMS Server*).
2. Access the Comtrend Boot Configurator by going to `<NMS_Home>/bin` and double-clicking on **AT_CTBootConfigurator**
3. On the Comtrend Boot Configurator Form (Figure 15-18), the only fields that must be filled in are:
   - Mgmt. VLAN
   - ACS URL: change the IP address to the NMS server used to manage the network

For a description of these and other fields, refer to Figure 15.6.5.

4. Uncheck the **Save Only** checkbox. Click on **OK**.
5. The CPE Connection dialog box opens Figure 15-23). Click OK. (Default Password is 12345.)


CPE Connection

Enter current CPE device login information

IP Address: 192.168.1.1

Login: root

Password: *****

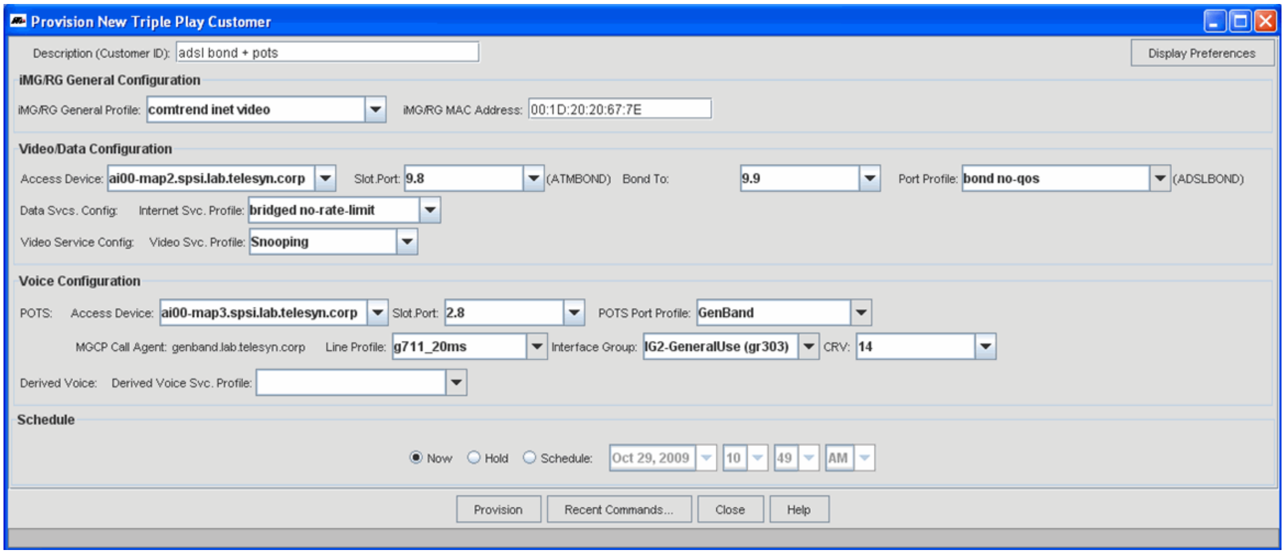
FIGURE 15-23 Comtrend CPE Connection Dialog Box

6. The configuration file is uploaded to the Comtrend device, the device reboots, and the device is now ready to be deployed.

15.6.9 Example Procedure - Provisioning

At an NMS client on the network, the Comtrend is provisioned as follows:

1. Bring up the Triple Play form for Bonded ports, as explained in "Provision a New Triple Play Customer" on page 398. Refer to Figure 15-24.
2. For the Comtrend device, you must enter a Description (Customer ID) of 15 characters or less. If more than 15 characters are used, the iMAP ADSL bond port will use the entire string, but the Comtrend CPE SysContact will be truncated to15 characters, resulting in more complex customer management.
3. For the Comtrend device, you must fill in the MAC address, found at the bottom of the Comtrend.
4. Do not use the Derived Voice-related fields, since derived voice will not be managed by the NMS (refer to "Feature Limitations" on page 512). *Note*: You may provision a POTS line.
5. Click on **Provision**. The Comtrend device is added to the iMG/RG table, but the IP address remains 0.0.0.0 until the Comtrend device is physically connected to the network.



Description (Customer ID): adsl bond + pots

iMG/RG General Configuration

iMG/RG General Profile: comtrend inet video iMG/RG MAC Address: 00:1D:20:20:67:7E

Video/Data Configuration

Access Device: ai00-map2.spsi.lab.telesyn.corp Slot.Port: 9.8 (ATMBOND) Bond To: 9.9 Port Profile: bond no-qos (ADSLBOND)

Data Svcs. Config: Internet Svc. Profile: bridged no-rate-limit

Video Service Config: Video Svc. Profile: Snooping

Voice Configuration

POTS: Access Device: ai00-map3.spsi.lab.telesyn.corp Slot.Port: 2.8 POTS Port Profile: GenBand

MGCP Call Agent: genband.lab.telesyn.corp Line Profile: g711_20ms Interface Group: IG2-GeneralUse (gr303) CRV: 14

Derived Voice: Derived Voice Svc. Profile:

Schedule

● Now ○ Hold ○ Schedule: Oct 29, 2009 10 49 AM

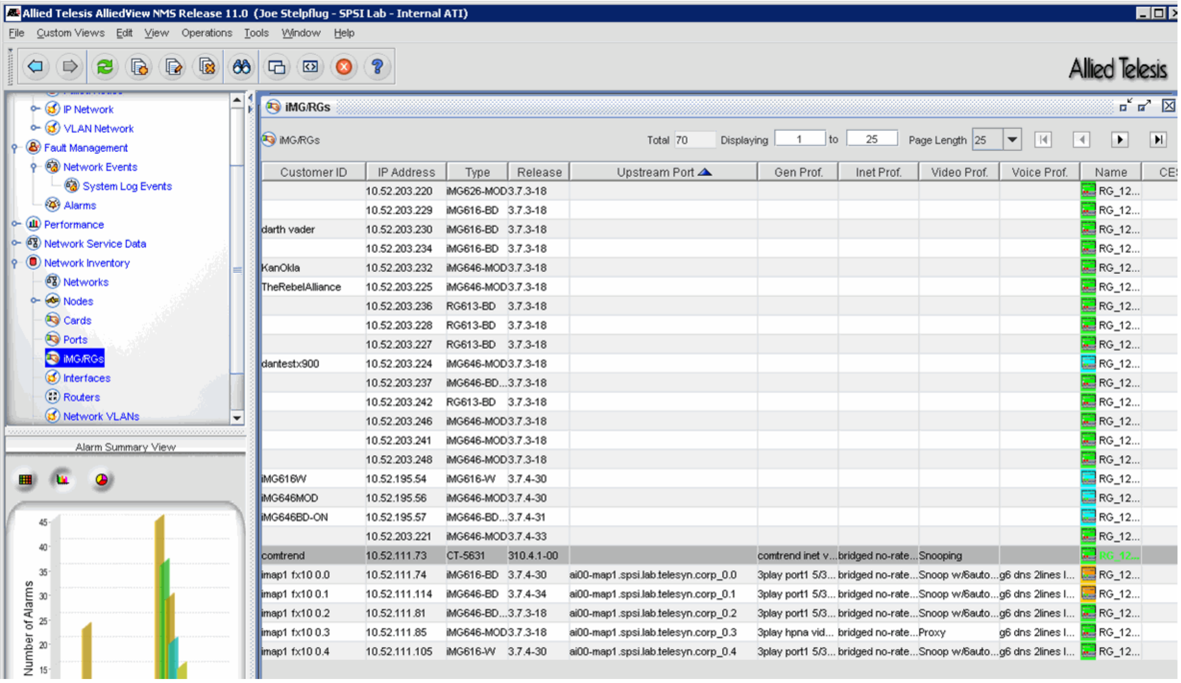
FIGURE 15-24 Triple Play Form for Comtrend Device

At the subscriber premises, the subscriber:

1. Plugs in the dual ADSL connection.
2. Powers up the Comtrend.

   The Comtrend boots up twice, first using the configuration parameters that were loaded during the staging process, and then the configuration downloaded by the NMS server. (This should take approximately five minutes.)
3. Connects the video and data devices. As the devices connect to the network, they come up and begin passing data.

Back at the NMS, on the iMG/RG table, the columns have provisioning information filled in, except for the upstream port, as shown in Figure 15-25.



iMG/RGs

Total 70 Displaying 1 to 25 Page Length 25

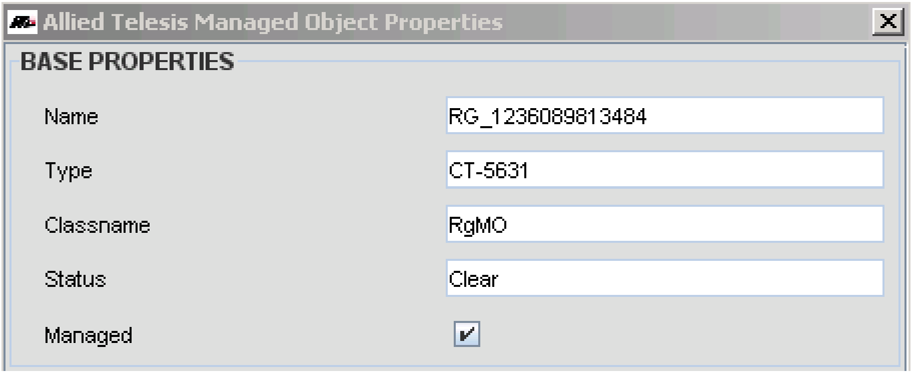
Customer ID	IP Address	Type	Release	Upstream Port	Gen Prof.	Inet Prof.	Video Prof.	Voice Prof.	Name	CE
	10.52.203.220	iMG626-MOD	3.7.3-18						RG_12...	
	10.52.203.229	iMG616-BD	3.7.3-18						RG_12...	
darth vader	10.52.203.230	iMG616-BD	3.7.3-18						RG_12...	
	10.52.203.234	iMG616-BD	3.7.3-18						RG_12...	
KanOkla	10.52.203.232	iMG646-MOD	3.7.3-18						RG_12...	
TheRebelAlliance	10.52.203.225	iMG646-MOD	3.7.3-18						RG_12...	
	10.52.203.236	RG613-BD	3.7.3-18						RG_12...	
	10.52.203.228	RG613-BD	3.7.3-18						RG_12...	
	10.52.203.227	RG613-BD	3.7.3-18						RG_12...	
dantestx900	10.52.203.224	iMG646-MOD	3.7.3-18						RG_12...	
	10.52.203.237	iMG646-BD...	3.7.3-18						RG_12...	
	10.52.203.242	RG613-BD	3.7.3-18						RG_12...	
	10.52.203.246	iMG646-MOD	3.7.3-18						RG_12...	
	10.52.203.241	iMG646-MOD	3.7.3-18						RG_12...	
	10.52.203.248	iMG646-MOD	3.7.3-18						RG_12...	
iMG616W	10.52.195.54	iMG616-W	3.7.4-30						RG_12...	
iMG646MOD	10.52.195.56	iMG646-MOD	3.7.4-30						RG_12...	
iMG646BD-ON	10.52.195.57	iMG646-BD...	3.7.4-31						RG_12...	
	10.52.203.221	iMG646-MOD	3.7.4-33						RG_12...	
comtrend	10.52.111.73	CT-5631	310.4.1-00		comtrend inet v...	bridged no-rate...	Snooping		RG_12...	
imap1 fx10 0.0	10.52.111.74	iMG616-BD	3.7.4-30	ai00-map1.spsi.lab.telesyn.corp_0.0	3play port1 5/3...	bridged no-rate...	Snoop w/6auto...	g6 dns 2lines l...	RG_12...	
imap1 fx10 0.1	10.52.111.114	iMG646-BD	3.7.4-34	ai00-map1.spsi.lab.telesyn.corp_0.1	3play port1 5/3...	bridged no-rate...	Snoop w/6auto...	g6 dns 2lines l...	RG_12...	
imap1 fx10 0.2	10.52.111.81	iMG646-BD...	3.7.3-18	ai00-map1.spsi.lab.telesyn.corp_0.2	3play port1 5/3...	bridged no-rate...	Snoop w/6auto...	g6 dns 2lines l...	RG_12...	
imap1 fx10 0.3	10.52.111.85	iMG646-MOD	3.7.3-18	ai00-map1.spsi.lab.telesyn.corp_0.3	3play hpna vid...	bridged no-rate...	Proxy	g6 dns 2lines l...	RG_12...	
imap1 fx10 0.4	10.52.111.105	iMG616-W	3.7.4-30	ai00-map1.spsi.lab.telesyn.corp_0.4	3play port1 5/3...	bridged no-rate...	Snoop w/6auto...	g6 dns 2lines l...	RG_12...	

FIGURE 15-25 Comtrend Device in iMG/RGs table

4. Go to the Nodes table and find the upstream iMAP device for the Comtrend. Right-click on the node, then click *Discover Attached iMG/RGs*. The Comtrend device now has the upstream port filled in at the iMG/RG table, and provisioning is complete.

15.6.10 Managed Object Properties

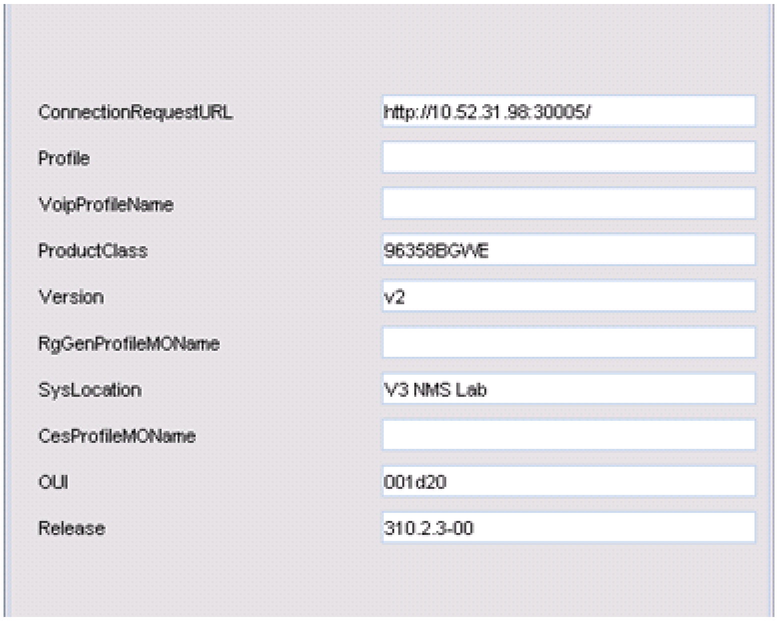
Right-click on the Comtrend row in the iMG/RG table. Selecting **Managed Object Properties** brings up the set of MO Properties window. The following figures show these.



BASE PROPERTIES

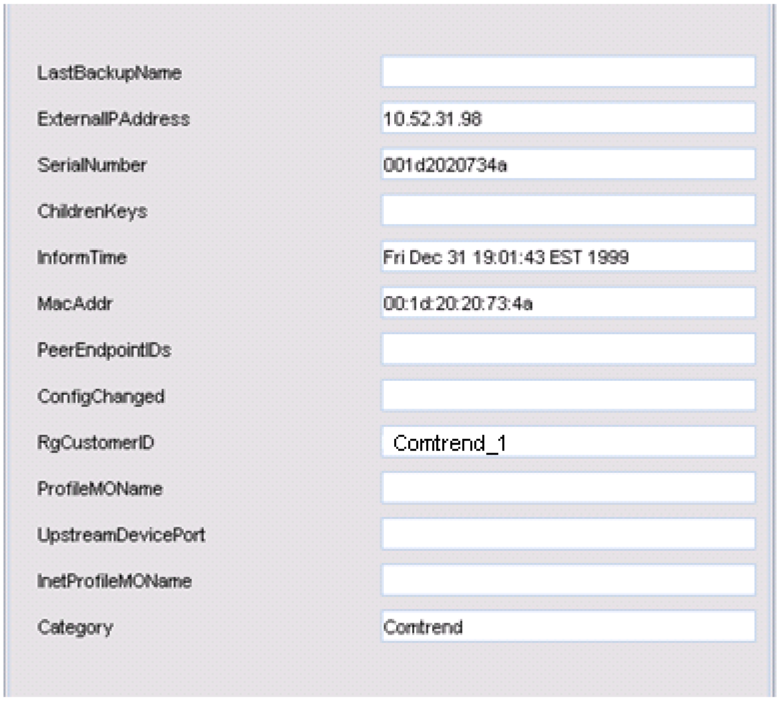
Name	RG_1236089813484
Type	CT-5631
Classname	RgMO
Status	Clear
Managed	☑

FIGURE 15-26 Comtrend Object Properties - Base



ConnectionRequestURL	http://10.52.31.98:30005/
Profile	
VoipProfileName	
ProductClass	96358BGWE
Version	v2
RgGenProfileMOName	
SysLocation	V3 NMS Lab
CesProfileMOName	
OUI	001d20
Release	310.2.3-00

FIGURE 15-27 Comtrend Device Parameters (1)



LastBackupName	
ExternalIPAddress	10.52.31.98
SerialNumber	001d2020734a
ChildrenKeys	
InformTime	Fri Dec 31 19:01:43 EST 1999
MacAddr	00:1d:20:20:73:4a
PeerEndpointIDs	
ConfigChanged	
RgCustomerID	Comtrend_1
ProfileMOName	
UpstreamDevicePort	
InetProfileMOName	
Category	Comtrend

FIGURE 15-28 Comtrend Device Parameters (2)

Several parameters are collected during discovery and by calling operations to retrieve basic device information and these few are required to manage the CPE using (CWMP) TR-069.

- Product Class - Group of devices differentiating device types
- OUI - Unique identifier for differentiating device category
- Connection Request URL - ACS initiated operations must use this URL
- Serial Number - Uniquely identifies the device to the NMS

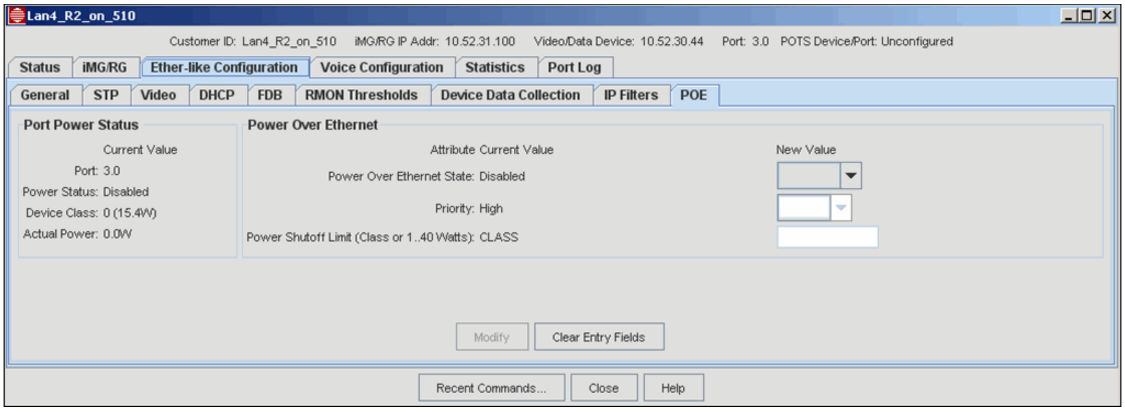
15.6.11 CWMP Browser

Also available in NMS release 11.0 SP5 is a CWMP browser that allows the user to view and change the parameters on a TR-069 compliant device. The tool is accessed by selecting *Tools -> CWMP Browser* (directly above SNMP MIB Browser). The TR-069 Operations Form appears.

In the Device pull-down are available TR-069 devices available for the NMS, which in release 11.0 SP5 are the Comtrend devices.

15.7 POE View / Modify Port

The Customer Management form has an additional POE tab that can be used to modify the POE settings for an individual port. Refer to the following figure.



Lan4_R2_on_510

Customer ID: Lan4_R2_on_510 iMG/RG IP Addr: 10.52.31.100 Video/Data Device: 10.52.30.44 Port: 3.0 POTS Device/Port: Unconfigured

Port Power Status

Current Value

Port: 3.0

Power Status: Disabled

Device Class: 0 (15.4W)

Actual Power: 0.0W

Power Over Ethernet

Attribute	Current Value	New Value
Power Over Ethernet State:	Disabled	
Priority:	High	
Power Shutoff Limit (Class or 1..40 Watts):	CLASS	

FIGURE 15-29 View / Modify POE Port

16. Configuring Network Services

You can use the NMS to configure network-based services.

16.1 Overview of Network Services

Table 16-1 lists the topics covered in this chapter.

TABLE 16-1 Network Services in AlliedView NMS Release 12.0

Network Service	Description	Notes / Section
Topology Maps and Inventory tables		"Topology Maps and Inventory Tables" on page 524
Network VLANs	Creating, Extending, and Trimming	"Creating Network VLANs" on page 533 through "Example of Creating Network VLANs" on page 550
HVLAN and VLAN Translation	Creating on iMAP interfaces	HVLAN - "HVLAN Configuration" on page 559 VLAN Translations - "VLAN Translations Configuration" on page 566
Protection Switching	Creating Control and Protected VLANs in a ring configuration (EPSR)	"Protection Switching-EPSR" on page 567
Protection Switching for SuperLoop	The EPSR feature is enhanced to include the SuperLoop feature.	"SuperLoop Prevention (Superring)" on page 596
Customer Provisioning	Allows network service features (Profiles, Quality of Service) to be incorporated when provisioning individual customers	"Customer Management" on page 615
Dual Endpoint CES8 Provisioning CES between CES8 and iMG6x6MOD	Allows two DS1/E1 endpoints to be provisioned simultaneously Allows T1/E1 LAN card in iMG to connect to CES8 port. (Two iMG6x6's can also interconnect.)	"Provision the Two DS1 Ports" on page 627 "Provisioning iMG6x6MOD with T1/E1 Card and CES" on page 636
Dual Endpoint NTE8 Provisioning	Allows two DS1/E1 endpoints to be provisioned simultaneously	"NTE8 Dual Circuit Provisioning" on page 653
UPC Monitoring	Displays Upstream Control Protocol (UCP) attributes for the VLAN submap and VLAN Interface Inventory	"Upstream Control Protocol (UCP) Display" on page 670

TABLE 16-1 Network Services in AlliedView NMS Release 12.0

Network Service	Description	Notes / Section
Link Discovery	A Physical link between devices will be automatically discovered if LLDP has been activated on its link ports at each end	New links are only updated during (re)discovery of the devices "LLDP Protocol and Associated Features (LAG/ VCS Monitoring)" on page 313 and "Link Discovery" on page 674
Software Upgrade support for EPSR and EPSR+	During upgrade of iMAP devices, nodes are updated in proper order to keep the EPSR ring in-service. If other nodes need to be added to upgrade sequence, GUIs appear.	If EPSR had not been configured correctly, a GUI with an error message appears. Refer to "Software Upgrade with EPSR" on page 675.
Diagnostic Audit	Provides the capability to run diagnostic audits on certain network entities. Currently, the auditable entities are: • Network VLANs • CES Circuits	Refer to "Diagnostic Audit" on page 682.
Port Authentication		Refer to "Port Authentication (802.1x)" on page 688.

16.1.1 Profile Management

Since most of the parameters in the configuration of certain ports or devices will be the same throughout the network, profile management is a way to set up these parameters (through profiles) and then apply them throughout the network in only a few steps and with less chance of error. Profile Management also allows the network administrator to easily re-deploy changes in a stored configuration to the devices/ports in the network. Finally, the AlliedView NMS allows the user to determine whether the configuration on a device or port still matches the configuration that was defined for it using Profile Management (and is therefore in-sync).

16.1.2 Quality of Service

The main strategy in providing QoS is to first classify and segregate traffic into separate flows. These flows can then be managed separately through the network with each flow getting a specified level of service.

The Rapier, Switchblade, and iMAP devices provide this function, with some variation between the device types. Refer to the User Guides for each device type for detailed information on how they provide QoS.

16.1.3 Protection Switching (EPSR)

The EPSR feature protects the parts of the network that have a ring topology. Key components that are configured are Control VLANs, Domains, and Protected VLANs.

A Control VLAN is configured on the set of devices, and is used to send and receive control messages over the ring network. The devices that are included in the control VLAN make up the Domain of the control VLAN.

The VLANs that require fault protection are configured on all the ring ports and are assigned to the EPSR domain. These VLANs are called Protected VLANs.

16.1.4 Circuit Emulation Service (CES)

The iMAP devices use the CES8 card to transport T1 point to point across an Ethernet network. This CES is in unstructured mode; in this mode, the CES8 creates a “pseudo-span” across the Ethernet network that acts like a virtual wire connection that accepts a bit stream into the pseudo-span, and recreates that same stream out of the pseudo-span.

When configuring CES, the user provisions through forms the functional components of the CES8 and iMAP device, as well as the network VLANs that connect devices and networks.

16.1.5 NTE8 Service

The NTE8 card allows DS1/E1 facilities to connect (backhaul) the ethernet network, with both ends of the DS1/E1 connections being on iMAP 9000 devices. Refer to the *Software Reference for iMAP Series Switches* for a complete description of the NTE8 configuration.

Note: Refer to "NTE8 Card" on page 389 and "NTE8 Port Management Form" on page 463 for an overview of the NTE8 card and DS1/E1 port attributes.

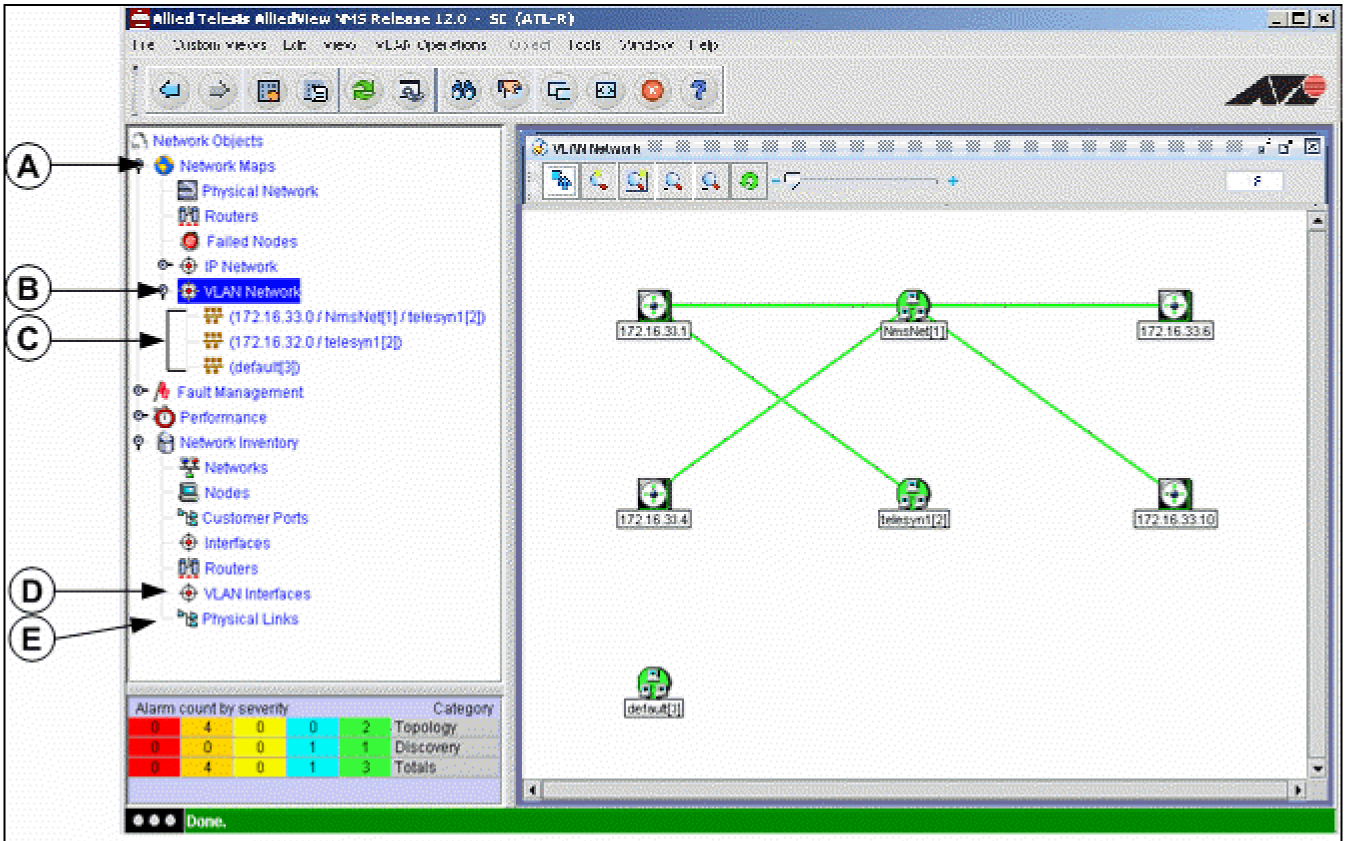
The NTE8 configuration always has dual endpoints, since there must be an iMAP 9000 device at each end. Moreover, each end must be correctly provisioned for the logical hierarchy (DS1, PPP, MLPP, ETH) of the NTE8. Finally, the hierarchy for each endpoint in a pair must be the same.

16.2 Topology Maps and Inventory Tables

To view and manipulate the network VLANs, a set of maps and tables show the configuration for the network VLANs and their status at the layer 3 and layer 2 for all their related components:

- The physical links that connect the devices
- The VLAN links that connect the VLAN interfaces
- The VLAN interfaces on the device
- The Network VLAN itself

The maps and tables that show these components are explained first, so that the menu items that create, change, and delete these components are more easily understood. Figure 16-1 shows the Network Objects node tree and highlights those that are used to view and configure network VLANs.



Alarm count by severity					Category
0	4	0	0	2	Topology
0	0	0	1	1	Discovery
0	4	0	1	3	Totals

A Physical connections between nodes

B VLAN network routing map (IP-based and island-based with layer-3 IP connectivity)

C VLAN network submaps (VLAN devices within one VLAN network and layer 2 connectivity)

D VLAN interfaces (device-level VLAN information)

E Physical links (Physical connections between devices

FIGURE 16-1 Network Objects used for Network VLANs

16.2.1 VLAN Network Map (Layer 3)

By containing symbols for routers and the layer 2 subnetworks, this map shows all VLAN networks and their Layer-3 (IP) connectivity.

On this map, an IP-based Network VLAN will include its router connections. An island-based Network VLAN will still appear as a layer 2 subnetwork symbol, but it will have no router connections. Refer to Figure 16-2.

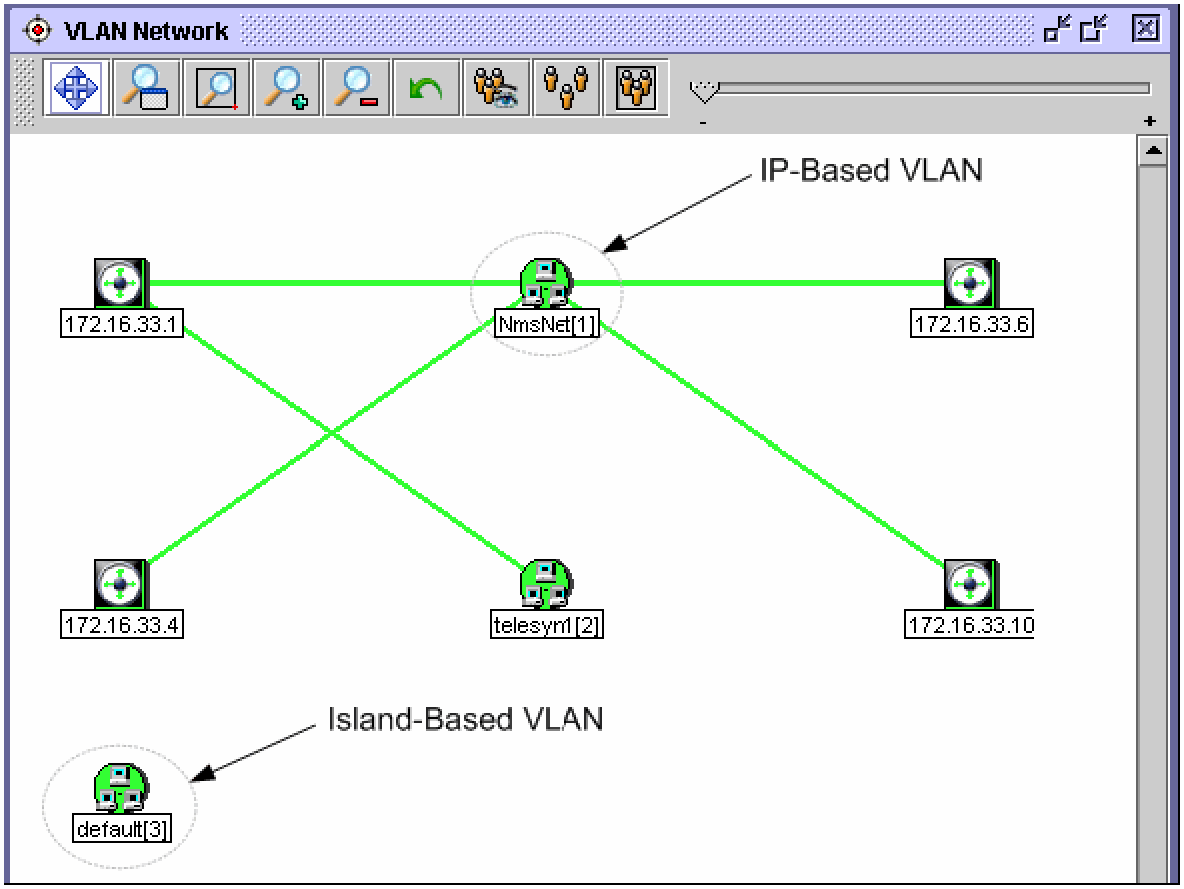


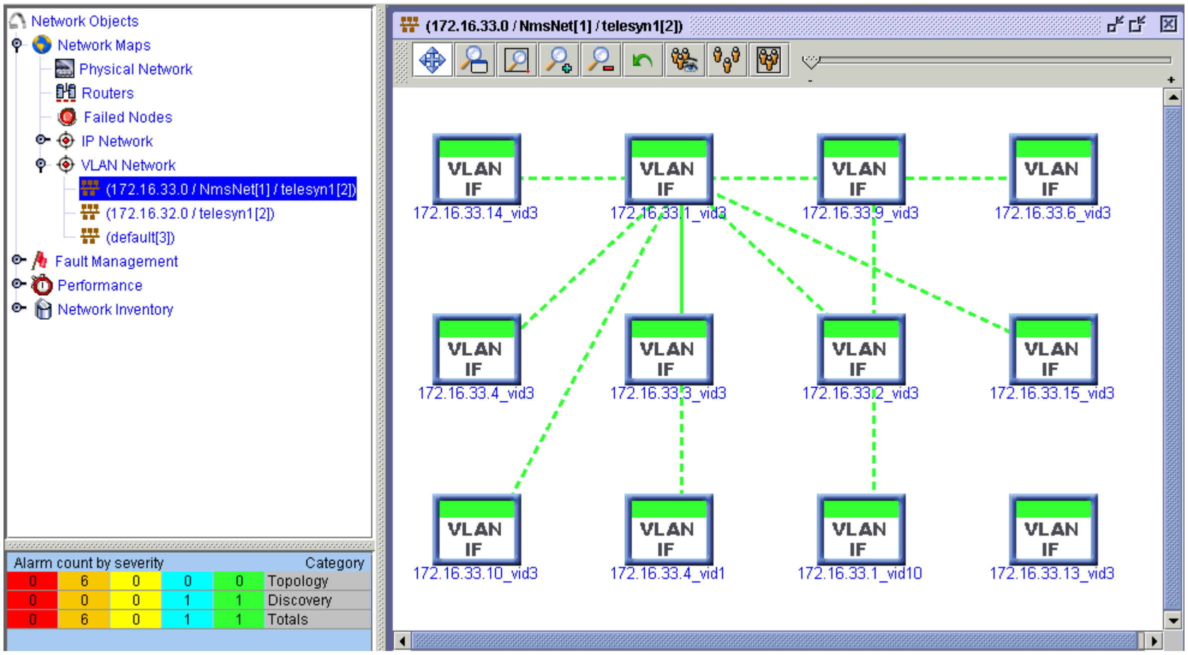
FIGURE 16-2 VLAN Network Map

Double-clicking any of the Network VLAN symbols or selecting one of the VLAN network nodes in the VLAN Network tree will open up the VLAN Network Map (layer 2), a map of the individual Network VLAN.

16.2.2 VLAN Sub Maps (Layer 2)

Each VLAN network symbol on the layer 3 topology map has its associated layer 2 topology map. These show the interfaces of the layer 2 subnetwork, as well as VLAN point-to-point connectivity (logical links) between the VLAN interfaces shown in Figure 16-3. On these maps the following tooltips are available:

- When over a link, the tooltip shows the VLAN link ID, which includes the VID and port numbers.
- When over a device, the tooltip shows the VLAN interface ID.



- Network Objects
  - Network Maps
    - Physical Network
    - Routers
    - Failed Nodes
    - IP Network
    - VLAN Network
      - (172.16.33.0 / NmsNet[1] / telesyn1[2])
      - (172.16.32.0 / telesyn1[2])
      - (default[3])
  - Fault Management
  - Performance
  - Network Inventory

Alarm count by severity					Category
0	6	0	0	0	Topology
0	0	0	1	1	Discovery
0	6	0	1	1	Totals

(172.16.33.0 / NmsNet[1] / telesyn1[2])

FIGURE 16-3 IVLAN Map (Layer 2)

Note: *The connectivity on the layer 2 VLAN subnetwork map is derived from the physical link connectivity that is configured and viewed in the Physical Network map. If physical links have been created on the Physical Networks map, the Network VLANs will appear here. This also allows Network VLANs to be configured even if the physical connections do not exist. Refer to "Physical Network Map" on page 527.*

The naming of the Network VLANs in the VLAN Network tree is as follows:

- For IP-based Network VLANs:

  <IP subnet>/<Network VLAN name>[<system-created number>]

  The system-created numbers in brackets are incremented whenever a Network VLAN is created. This ensures that VLANs created with the same name can be identified. Also, there can be more than one Network VLAN on an IP submap if there are two separate Network VLANs within the same IP address.

- For island-based VLANS:

  <Network VLAN name>[<system-created number in brackets>]

When a VLAN submap is the active panel, the VLAN Operations menu pull-down appears and the following options are available:

- Delete VLAN - Refer to "Deleting Network VLANs" on page 542.
- Map Properties.

16.2.3 Physical Network Map

This map shows all of the physical devices that have been discovered, as well as the physical connections that exist between the devices. For all physical connection(s) between physical devices, a single line will appear.

Note: *Since the physical connection between devices may contain one or more physical links, the connection is referred to as a linkset.This is explained later in this subsection.*

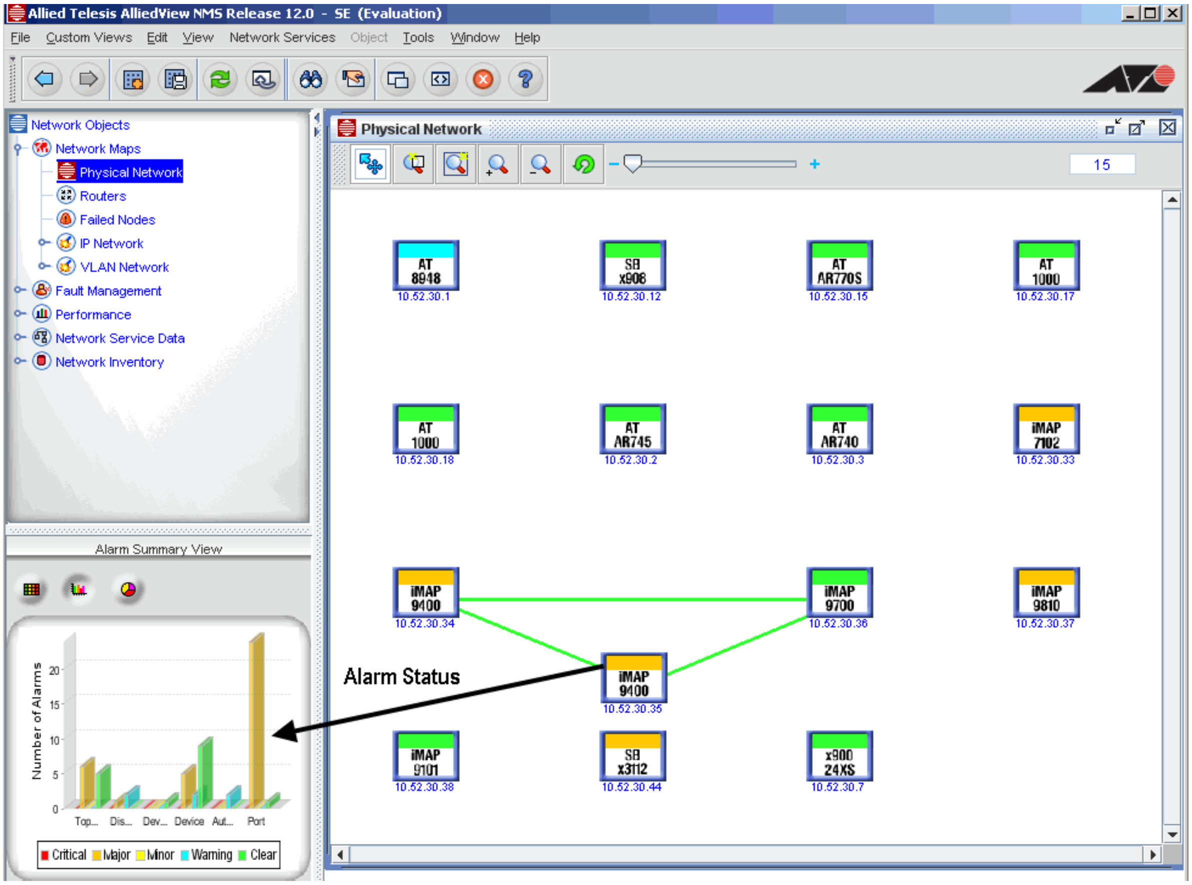


FIGURE 16-4 Physical Network Map

The ability to add, delete, and view physical links is useful in the following scenarios:

- Viewing existing Network VLANs - As the physical connections are created and configured, if there is an existing Network VLAN that uses that physical connection, its submap will automatically be configured and added to the VLAN Network nodes.
- Creating Network VLANs - If the physical connections exist, the options available on this map are used to create a Network VLAN. Devices can be chosen and the Network VLAN GUI Wizard can be used to create and configure a Network VLAN. Refer to "Creating Initial VLAN Information" on page 533.
- Modeling Network VLANs for study - A physical connection can be created that does not actually exist, and then a VLAN configuration can be associated with it. This allows Network Administrators to study the Network VLAN and ensure it follows the topology they desire before connecting the physical link.

This map also shows the status of the devices and links and if any alarms are present. Refer to "Alarm Indicators from the Maps and Inventory Tables" on page 533.

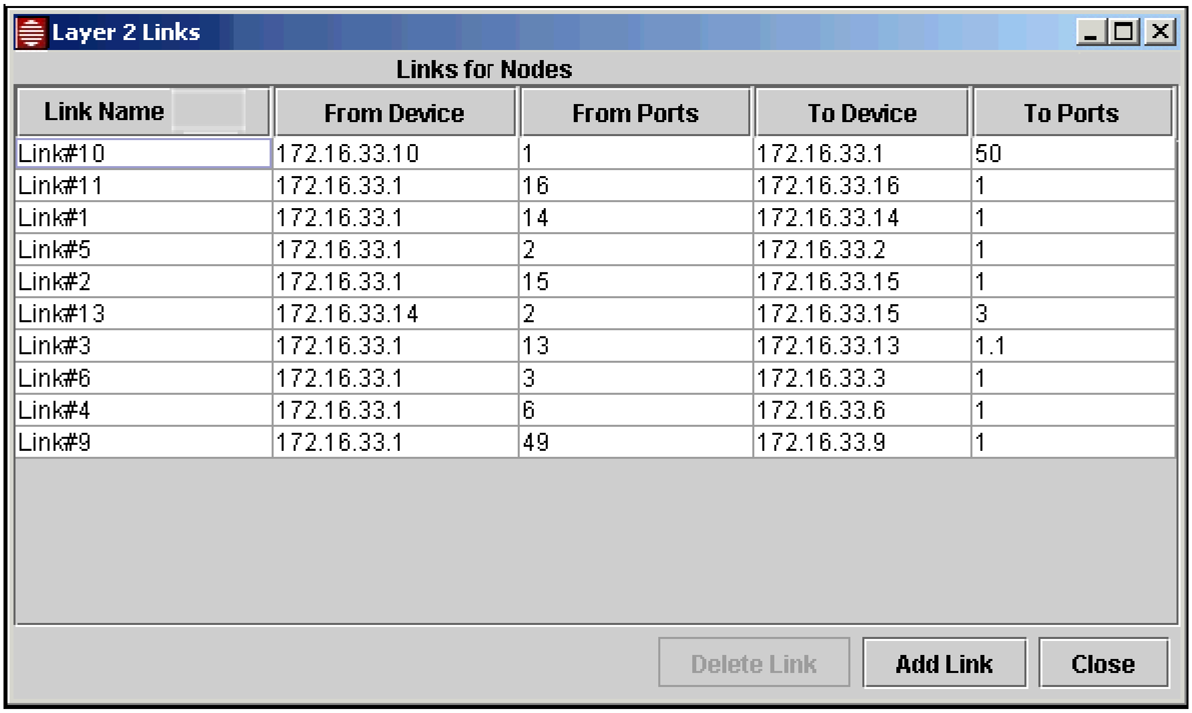
When the Physical Network map is the active panel, the **Network Services** menu pull-down appears and the following options are available. (These also appear when you right-click the device.)

- Link Operations - Used to add and delete links between two nodes. Refer to Figure 16-7.
- VLAN - Accesses a submenu that includes the following:
  - Create VLAN - Creates a Network VLAN and all of its components
  - Show VLANs - Lists the Name, ID, and subnets for all Network VLANs
  - Delete VLAN - Delete a Network VLAN

- Network VLAN Manager - Shows all Network VLANs in a hierarchy

To create a physical link, select *Network Service -> Link Operations* from the pull-down menu or right click anywhere on the map area. The Layer 2 Links form appears, as shown in Figure 16-5. This form displays the links associated with the Nodes and/or Links that are currently selected. If no links are selected, it displays all Links in the NMS database. These forms will also reflect any changes made from other forms and even other NMS Clients

Note: *A single visible line between two devices on the Physical Networks map may represent one or more than one link. (Double-clicking on the link will show the number of links.) Therefore, a link symbol on the map is properly called a linkset, so when creating a physical link you are actually creating one of the links in the linkset. This is important when creating model VLANs, since they use physical links that do not actually exist. When creating a model physical link (does not actually exist), it is recommended to go to the Physical Links table in Network Inventory and UnManage that link. Doing this will unmanage any associated model VLAN links causing them to be displayed with a gray color, which indicates that they are modeled links.*



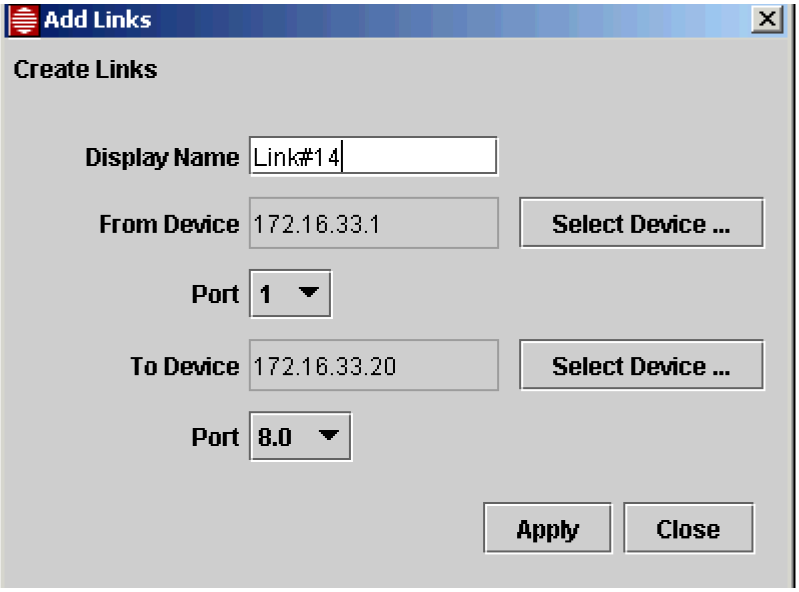
Links for Nodes

Link Name	From Device	From Ports	To Device	To Ports
Link#10	172.16.33.10	1	172.16.33.1	50
Link#11	172.16.33.1	16	172.16.33.16	1
Link#1	172.16.33.1	14	172.16.33.14	1
Link#5	172.16.33.1	2	172.16.33.2	1
Link#2	172.16.33.1	15	172.16.33.15	1
Link#13	172.16.33.14	2	172.16.33.15	3
Link#3	172.16.33.1	13	172.16.33.13	1.1
Link#6	172.16.33.1	3	172.16.33.3	1
Link#4	172.16.33.1	6	172.16.33.6	1
Link#9	172.16.33.1	49	172.16.33.9	1

FIGURE 16-5 Layer 2 Links Form

Note: *This Form also inlcudes Link Type, Discoverd By, and Parent Link. Refer to "Port Authentication (802.1x)" on page 688 for an example that uses these columns.*

From this list, the Add Link button is used to create a link between two devices. The **Add Links** form appears, as shown in Figure 16-6.



Add Links

Create Links

Display Name: Link#14

From Device: 172.16.33.1

Port: 1

To Device: 172.16.33.20

Port: 8.0

FIGURE 16-6 Add Links Form for a Physical Connection

From this form, enter the name that will be given to the link. Use the **Select Device** to select which devices will be the end points of the link. Once the devices are selected, the available ports are shown in the pull-down menu for the Port. When the **Apply** button is clicked, the new link is automatically added to the Layer 2 Links table.

A link can also be deleted using the Layer 2 Links form. Once a link is highlighted, the Delete button is enabled, and the link can be deleted.

Note: When deleting a physical link, be aware that if the link is carrying logical VLAN links, these will be deleted from the VLAN submaps. Deleting links will not have any impact on the devices themselves.

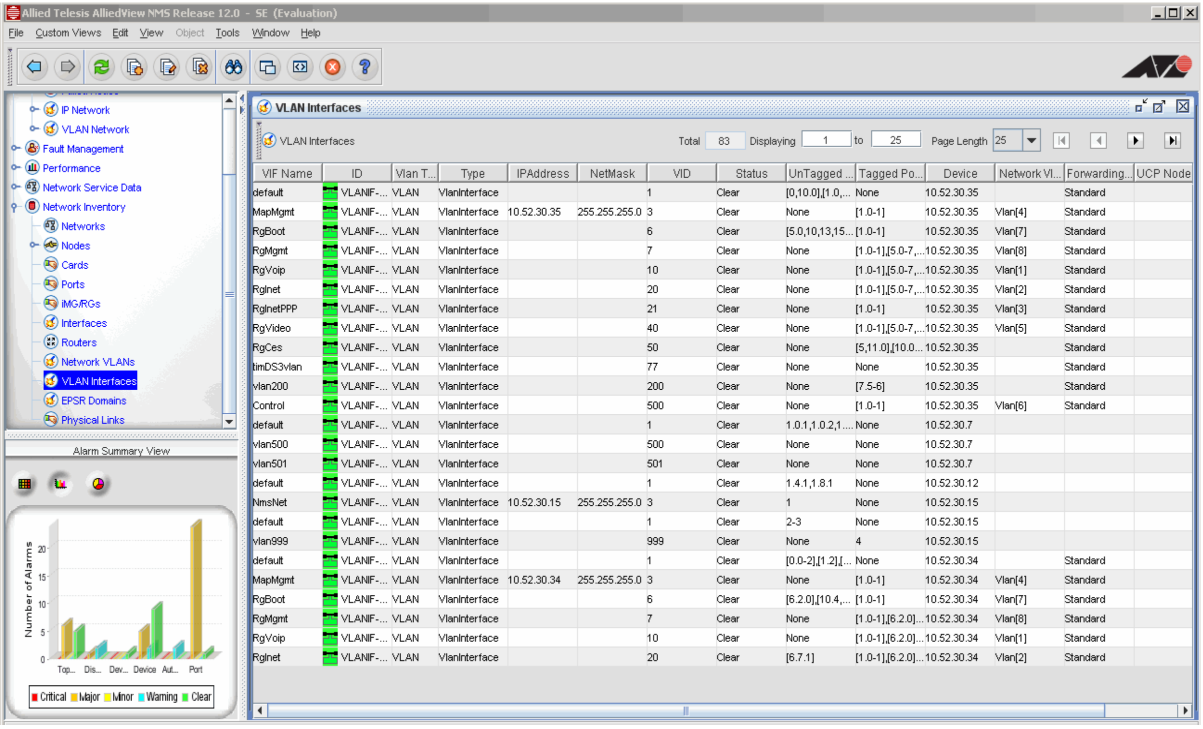
When a specific link is highlighted, the ***Physical Link*** pull-down appears and the following options are available:

- *Link Operations* - This invokes the Layer 2 Links form.
- *Show VLANs* - Show all the Network VLANs that use the link.
- *Properties* -The symbol properties.
- Managed Object Properties - The MO properties.
- Manage/UnManage - Makes the device managed or unmanaged by the AlliedView NMS.
- Update Status - The AlliedView NMS polls the link for its status.

16.2.4 VLAN Interfaces Inventory Table

In the Network Inventory Objects tree, the VLAN Interfaces table lists the inventory for all VLAN IFs. Like all inventory panels, it can be sorted by column (by clicking on the column head), and the number of rows listed can be controlled. Also, the entire table or selected rows can be exported to an external file or to your Web browser.

Figure 16-7 shows the Network Inventory Table for VLAN Interfaces, while Table 16-2 describes the columns.



Total 83 Displaying 1 to 25 Page Length 25

VIF Name	ID	Vlan T...	Type	IPAddress	NetMask	VID	Status	UnTagged ...	Tagged Po...	Device	Network Vl...	Forwarding...	UCP Node
default	VLANIF-...	VLAN	VlanInterface			1	Clear	[0,10.0],[1.0,...	None	10.52.30.35		Standard	
MapMgmt	VLANIF-...	VLAN	VlanInterface	10.52.30.35	255.255.255.0	3	Clear	None	[1.0-1]	10.52.30.35	Vlan[4]	Standard	
RgBoot	VLANIF-...	VLAN	VlanInterface			6	Clear	[5.0,10,13,15...	[1.0-1]	10.52.30.35	Vlan[7]	Standard	
RgMgmt	VLANIF-...	VLAN	VlanInterface			7	Clear	None	[1.0-1],[5.0-7,...	10.52.30.35	Vlan[8]	Standard	
RgVoip	VLANIF-...	VLAN	VlanInterface			10	Clear	None	[1.0-1],[5.0-7,...	10.52.30.35	Vlan[1]	Standard	
RgInet	VLANIF-...	VLAN	VlanInterface			20	Clear	None	[1.0-1],[5.0-7,...	10.52.30.35	Vlan[2]	Standard	
RgInetPPP	VLANIF-...	VLAN	VlanInterface			21	Clear	None	[1.0-1]	10.52.30.35	Vlan[3]	Standard	
RgVideo	VLANIF-...	VLAN	VlanInterface			40	Clear	None	[1.0-1],[5.0-7,...	10.52.30.35	Vlan[5]	Standard	
RgCes	VLANIF-...	VLAN	VlanInterface			50	Clear	None	[5,11.0],[10.0...	10.52.30.35		Standard	
timDS3vlan	VLANIF-...	VLAN	VlanInterface			77	Clear	None	None	10.52.30.35		Standard	
vlan200	VLANIF-...	VLAN	VlanInterface			200	Clear	None	[7.5-6]	10.52.30.35		Standard	
Control	VLANIF-...	VLAN	VlanInterface			500	Clear	None	[1.0-1]	10.52.30.35	Vlan[6]	Standard	
default	VLANIF-...	VLAN	VlanInterface			1	Clear	1.0.1,1.0.2,1....	None	10.52.30.7			
vlan500	VLANIF-...	VLAN	VlanInterface			500	Clear	None	None	10.52.30.7			
vlan501	VLANIF-...	VLAN	VlanInterface			501	Clear	None	None	10.52.30.7			
default	VLANIF-...	VLAN	VlanInterface			1	Clear	1.4.1,1.8.1	None	10.52.30.12			
NmsNet	VLANIF-...	VLAN	VlanInterface	10.52.30.15	255.255.255.0	3	Clear	1	None	10.52.30.15			
default	VLANIF-...	VLAN	VlanInterface			1	Clear	2-3	None	10.52.30.15			
vlan999	VLANIF-...	VLAN	VlanInterface			999	Clear	None	4	10.52.30.15			
default	VLANIF-...	VLAN	VlanInterface			1	Clear	[0.0-2],[1.2],[...	None	10.52.30.34		Standard	
MapMgmt	VLANIF-...	VLAN	VlanInterface	10.52.30.34	255.255.255.0	3	Clear	None	[1.0-1]	10.52.30.34	Vlan[4]	Standard	
RgBoot	VLANIF-...	VLAN	VlanInterface			6	Clear	[6.2.0],[10.4,...	[1.0-1]	10.52.30.34	Vlan[7]	Standard	
RgMgmt	VLANIF-...	VLAN	VlanInterface			7	Clear	None	[1.0-1],[6.2.0]...	10.52.30.34	Vlan[8]	Standard	
RgVoip	VLANIF-...	VLAN	VlanInterface			10	Clear	None	[1.0-1],[6.2.0]...	10.52.30.34	Vlan[1]	Standard	
RgInet	VLANIF-...	VLAN	VlanInterface			20	Clear	[6.7.1]	[1.0-1],[6.2.0]...	10.52.30.34	Vlan[2]	Standard	

FIGURE 16-7 Network Inventory for VLAN Interfaces

TABLE 16-2 VLAN Interfaces Inventory Table

Column	Description
VLAN Interface Name	The name of the VLAN interface on the device, which can be specified when creating a Network VLAN using the GUI wizard. Refer to "Creating Initial VLAN Information" on page 533.
ID	The VLAN interface ID (device name and VLAN ID).
Type	The type of interface. Always VlanInterface in this inventory table.
IPAddress	If the VLAN Interface is IP-based, its subnetwork.
NetMask	The net mask for the subnetwork.
VID	The VLAN ID number.
Status	Alarm Status. If no alarms, the status is Clear.
Untagged Ports	On the device, the ports that are labeled as untagged for the VLAN.
Tagged Ports	On the device, the ports that are labeled as tagged for the VLAN.
Device	The device name.
Network VLAN	The network VLAN to which this VLAN interface belongs.

When the VLAN Interfaces Inventory table is the active panel and one row is selected, the *VLAN Interface* menu pull-down appears and the following options are available:

- *Configure VLAN Interface* - This brings up the **VLAN Interface Configuration** form, and allows VLANs to be configured on the individual device. This is the same form displayed when provisioning a device, and is described in "Configure VLAN (Chassis View)" on page 335.
- *Extend VLAN* - This is described in "Extending Network VLANs" on page 539.

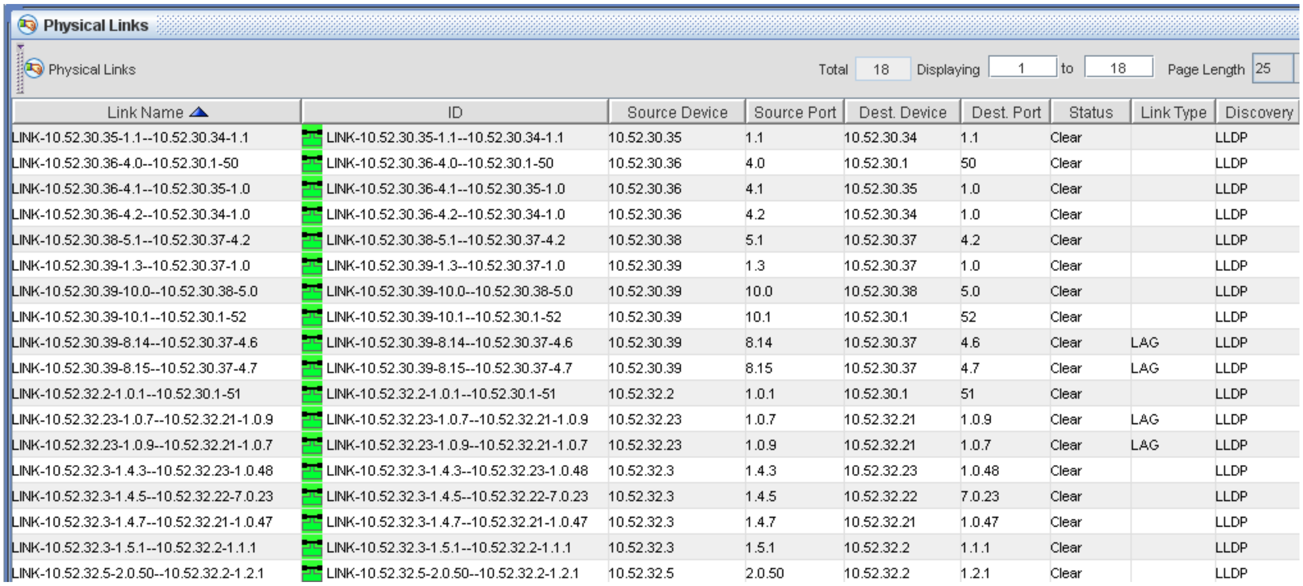
- *Alarms/Events* - This will invoke the Fault Management tables for Alarms and Events specific to the VLAN IF.
- *Managed Object Properties* - The base properties of the interface, including the IP address and netmask if it is part of a VLAN.
- *Delete Object and Traces* - This will delete the VLAN IF and all its sub-elements, so there is a confirmation window.
- *Manage/UnManage* - The interface will (or will no longer) be polled by the AlliedView NMS. The color of the row icon turns to gray.
- *Update Status* - The AlliedView NMS polls the device for its status.

16.2.5 Physical Links Inventory Table

For any physical link that is created from the Physical Network map or already exists, there is a row in this table.

Like all inventory panels, it can be sorted by column (by clicking column heading), and the number of rows listed can be controlled. Also, the entire table or selected rows can be exported to an external file or to your Web browser

Figure 16-8 shows the Network Inventory Table for VLAN Interfaces, while Table 16-3 describes the columns.



Link Name ▲	ID	Source Device	Source Port	Dest. Device	Dest. Port	Status	Link Type	Discovery
LINK-10.52.30.35-1.1--10.52.30.34-1.1	🟩 LINK-10.52.30.35-1.1--10.52.30.34-1.1	10.52.30.35	1.1	10.52.30.34	1.1	Clear		LLDP
LINK-10.52.30.36-4.0--10.52.30.1-50	🟩 LINK-10.52.30.36-4.0--10.52.30.1-50	10.52.30.36	4.0	10.52.30.1	50	Clear		LLDP
LINK-10.52.30.36-4.1--10.52.30.35-1.0	🟩 LINK-10.52.30.36-4.1--10.52.30.35-1.0	10.52.30.36	4.1	10.52.30.35	1.0	Clear		LLDP
LINK-10.52.30.36-4.2--10.52.30.34-1.0	🟩 LINK-10.52.30.36-4.2--10.52.30.34-1.0	10.52.30.36	4.2	10.52.30.34	1.0	Clear		LLDP
LINK-10.52.30.38-5.1--10.52.30.37-4.2	🟩 LINK-10.52.30.38-5.1--10.52.30.37-4.2	10.52.30.38	5.1	10.52.30.37	4.2	Clear		LLDP
LINK-10.52.30.39-1.3--10.52.30.37-1.0	🟩 LINK-10.52.30.39-1.3--10.52.30.37-1.0	10.52.30.39	1.3	10.52.30.37	1.0	Clear		LLDP
LINK-10.52.30.39-10.0--10.52.30.38-5.0	🟩 LINK-10.52.30.39-10.0--10.52.30.38-5.0	10.52.30.39	10.0	10.52.30.38	5.0	Clear		LLDP
LINK-10.52.30.39-10.1--10.52.30.1-52	🟩 LINK-10.52.30.39-10.1--10.52.30.1-52	10.52.30.39	10.1	10.52.30.1	52	Clear		LLDP
LINK-10.52.30.39-8.14--10.52.30.37-4.6	🟩 LINK-10.52.30.39-8.14--10.52.30.37-4.6	10.52.30.39	8.14	10.52.30.37	4.6	Clear	LAG	LLDP
LINK-10.52.30.39-8.15--10.52.30.37-4.7	🟩 LINK-10.52.30.39-8.15--10.52.30.37-4.7	10.52.30.39	8.15	10.52.30.37	4.7	Clear	LAG	LLDP
LINK-10.52.32.2-1.0.1--10.52.30.1-51	🟩 LINK-10.52.32.2-1.0.1--10.52.30.1-51	10.52.32.2	1.0.1	10.52.30.1	51	Clear		LLDP
LINK-10.52.32.23-1.0.7--10.52.32.21-1.0.9	🟩 LINK-10.52.32.23-1.0.7--10.52.32.21-1.0.9	10.52.32.23	1.0.7	10.52.32.21	1.0.9	Clear	LAG	LLDP
LINK-10.52.32.23-1.0.9--10.52.32.21-1.0.7	🟩 LINK-10.52.32.23-1.0.9--10.52.32.21-1.0.7	10.52.32.23	1.0.9	10.52.32.21	1.0.7	Clear	LAG	LLDP
LINK-10.52.32.3-1.4.3--10.52.32.23-1.0.48	🟩 LINK-10.52.32.3-1.4.3--10.52.32.23-1.0.48	10.52.32.3	1.4.3	10.52.32.23	1.0.48	Clear		LLDP
LINK-10.52.32.3-1.4.5--10.52.32.22-7.0.23	🟩 LINK-10.52.32.3-1.4.5--10.52.32.22-7.0.23	10.52.32.3	1.4.5	10.52.32.22	7.0.23	Clear		LLDP
LINK-10.52.32.3-1.4.7--10.52.32.21-1.0.47	🟩 LINK-10.52.32.3-1.4.7--10.52.32.21-1.0.47	10.52.32.3	1.4.7	10.52.32.21	1.0.47	Clear		LLDP
LINK-10.52.32.3-1.5.1--10.52.32.2-1.1.1	🟩 LINK-10.52.32.3-1.5.1--10.52.32.2-1.1.1	10.52.32.3	1.5.1	10.52.32.2	1.1.1	Clear		LLDP
LINK-10.52.32.5-2.0.50--10.52.32.2-1.2.1	🟩 LINK-10.52.32.5-2.0.50--10.52.32.2-1.2.1	10.52.32.5	2.0.50	10.52.32.2	1.2.1	Clear		LLDP

FIGURE 16-8 Physical Links Inventory Table

TABLE 16-3 Physical Links Inventory Table

Column	Description
Link Name	The name given when creating a Network VLAN using the GUI wizard.
ID	The physical link ID (device names and port numbers at each end of the link).
Source Device	The name of the source device.
Source Port	The physical port on the source device.
Dest. Device	The name of the destination device.
Dest. Port	The physical port on the destination device.
Status	Alarm Status. If no alarms, the status is Clear.

TABLE 16-3 Physical Links Inventory Table

Column	Description
Link Type	Specifies if the link provides a feature, such as LAG
Discovery	The protocol used to discover the link, such as LLDP

When the Physical Links table is the active panel, the *Link* menu pull-down appears and the following options are available:

- *Managed Object Properties* - The base properties of the physical link.
- *Alarms/Events* - This will invoke the Fault Management tables for Alarms and Events on the selected link.
- *Manage/UnManage* - The link may be set to unmanaged to indicate that it is not a real link, but rather a modelled link. The color of the link will be gray and the link will not change status based on alarms.

Note: *As mentioned in "Physical Network Map" on page 527, when creating a model physical link (does not actually exist), it is recommended to go to the Physical Links table in Network Inventory and UnManage that link. Doing this will unmanage any associated model VLAN links.*

- *Update Status* - The AlliedView NMS checks the alarm database for its status. The status is updated automatically, so this update status request should not be necessary for links.

16.2.6 Alarm Indicators from the Maps and Inventory Tables

When there is an alarm condition for any component in the network VLAN configuration, the following categories of alarms may be raised:

- Port
- VLAN IF
- Link
- Discovery
- Topology

For any component in any map or table, right-clicking the component brings up the Network Events or Alarms table for only that component and the condition can be examined more closely.

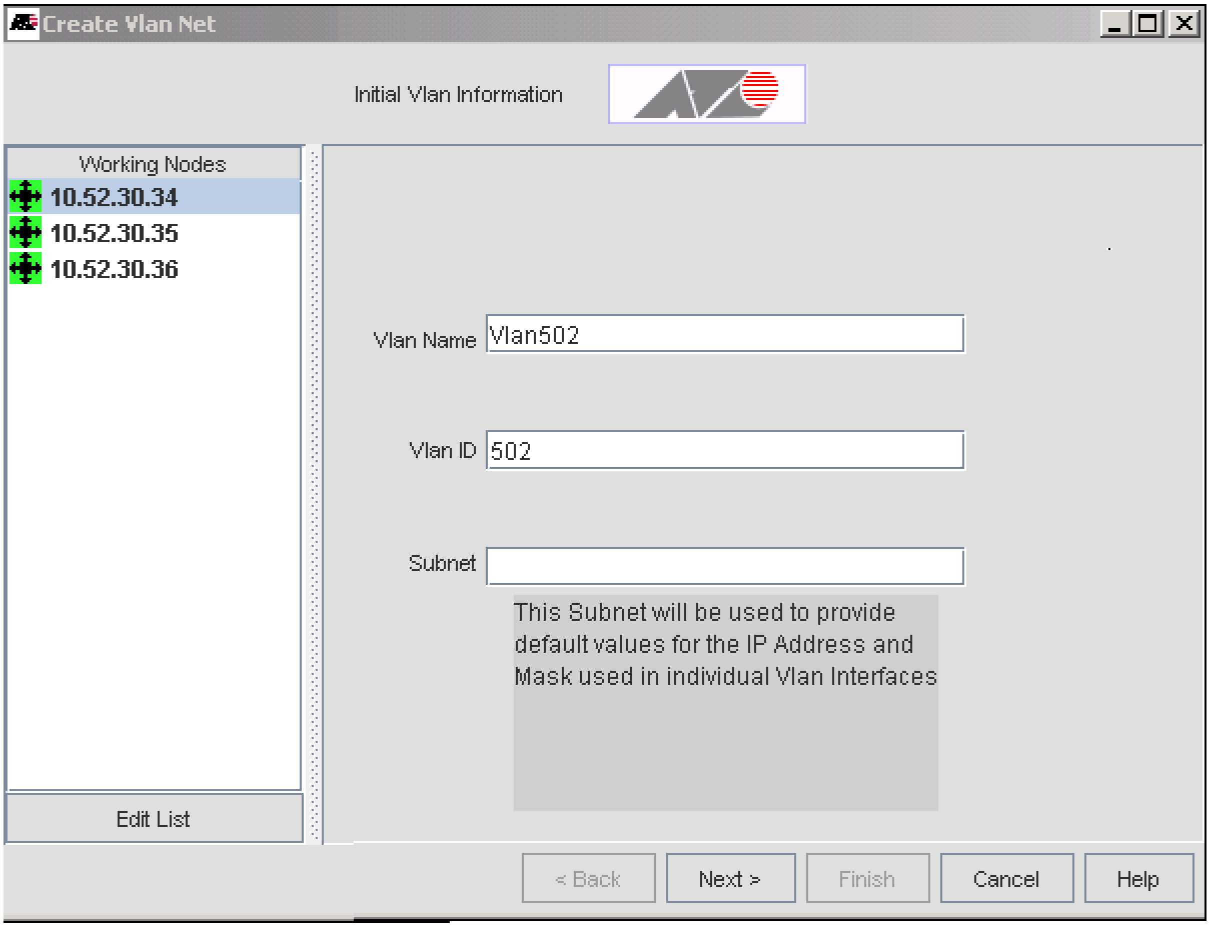
16.3 Creating Network VLANs

From the Physical Network map, a Network VLAN can be created using a GUI wizard that goes through all of the steps to create all of the needed components.

Note: *The user can also highlight a VLAN that already exists in the VLAN Network node and right click; all of the VLAN tasks are accessible.*

16.3.1 Creating Initial VLAN Information

To create a network VLAN, select one or more nodes on the Physical Network map. This can be done by clicking one node, and then holding down the Shift key while selecting other nodes. Links between nodes can be selected as well. Select *Network Services -> VLAN -> Create VLAN* from the pull-down menu, or right-click one of the nodes. The **Create VLAN Net** form will appear, as shown in Figure 16-9. The form will be pre-populated with the selected nodes and links. Table 16-4 shows the options available.



Vlan Name: Vlan502

Vlan ID: 502

Subnet:

This Subnet will be used to provide default values for the IP Address and Mask used in individual Vlan Interfaces

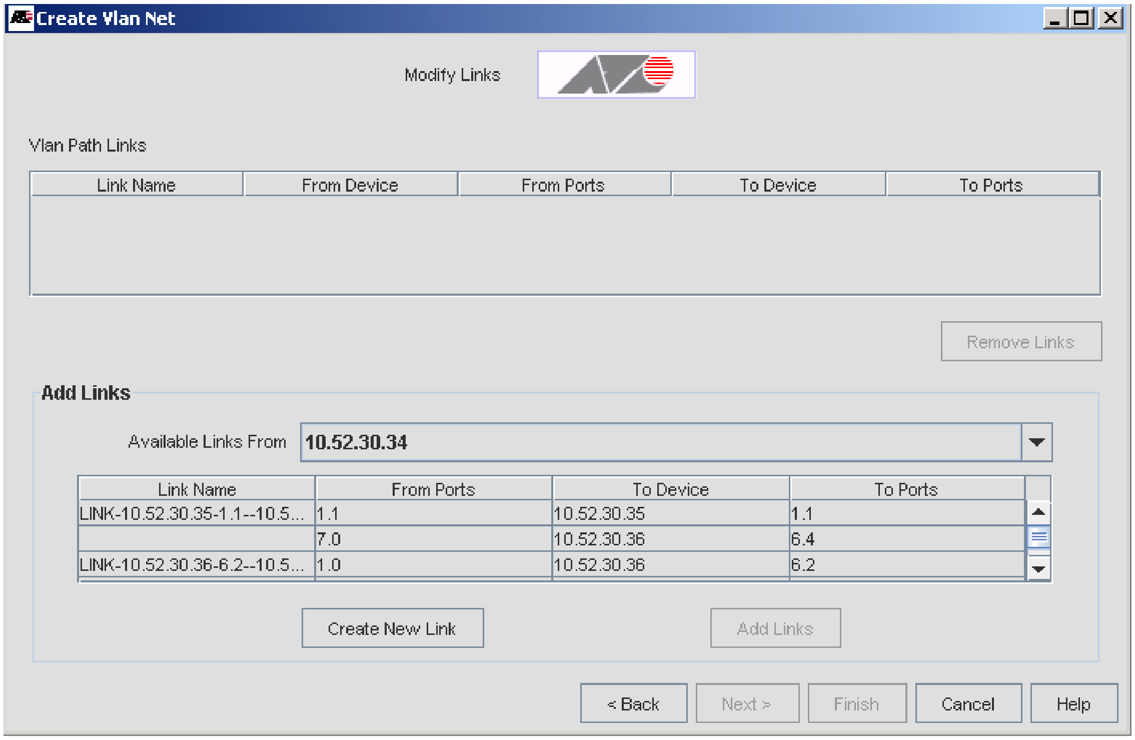
FIGURE 16-9 Create VLAN Net Form - Initial VLAN Information

TABLE 16-4 Create VLAN Net Form

Column	Description
Working Nodes	Nodes that are to be included in the Network VLAN. Nodes not in the original working nodes can be included in a VLAN by following an existing or newly created link to a new node. This is not recommended, though, as the auto-selected VLAN ID and VLAN Name may clash with entries already on these new nodes. To add or delete nodes, select **Edit List**.
Vlan Name	The name for the Network VLAN. This is usually descriptive text and includes the VID. The default is Vlan and a number selected by the AlliedView NMS.
Vlan ID (VID)	The VLAN ID number. This VID will be applied to each device VLAN interface during creation.
subNet	If this Network VLAN is to be IP-based, enter the subnetwork and the mask bitset, such as 172.16.32.0/24. If this field is left blank, an island-based Network VLAN is being created.
Next	If there are Working Nodes and at least the Vlan and VID fields are filled, clicking this button goes to the next form. (The Back and Finish buttons are always disabled in this initial form.)
Cancels	Dismisses the form and saves no data.

16.3.2 Modify the Network VLAN Link Configuration

Once **Next** is clicked, the VLAN links (and the physical links that they go over) can be added, changed, or removed. This is done with the **Modify Links** form, as shown in the following figure.



Link Name	From Device	From Ports	To Device	To Ports

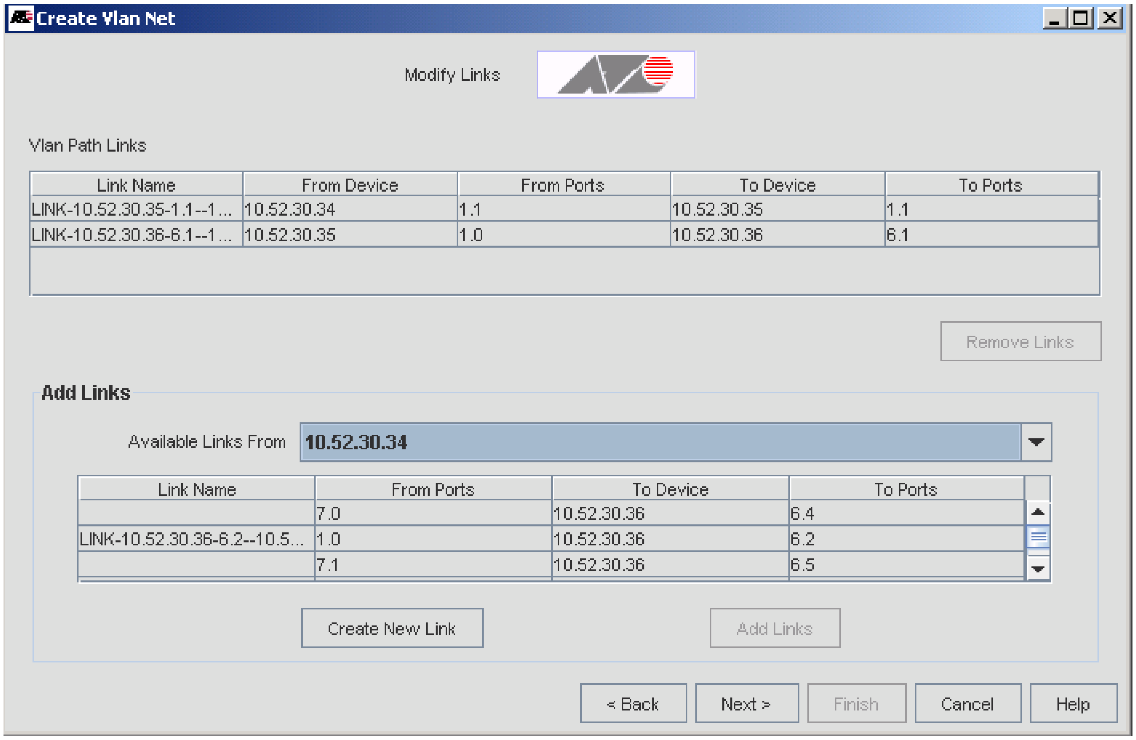
Available Links From 10.52.30.34

Link Name	From Ports	To Device	To Ports
LINK-10.52.30.35-1.1--10.5...	1.1	10.52.30.35	1.1
	7.0	10.52.30.36	6.4
LINK-10.52.30.36-6.2--10.5...	1.0	10.52.30.36	6.2

FIGURE 16-10 Create VLAN Net Form - Modify Links

Any links that were selected from the Physical Map when the Wizard was started are displayed in the **Vlan Path Links** table on this form. The available physical links from each device are listed in the **Add Links** subform. Selecting the desired link from the Add Links list and then clicking **Add Links** (now active) will place the selected link as one of the VLAN Path links, as shown in Figure 16-11.

Note: When a link from one device is added to the VLAN Path Links, the next device is selected in the Add Links subform. This would follow the normal procedure of going to the next "hop" in the Network VLAN. This procedure allows one to "walk" from one device to the next over the interconnecting physical links, resulting in a connected set VLAN interface that will form the broadcast domain of the created VLAN.



Vlan Path Links

Link Name	From Device	From Ports	To Device	To Ports
LINK-10.52.30.35-1.1--1...	10.52.30.34	1.1	10.52.30.35	1.1
LINK-10.52.30.36-6.1--1...	10.52.30.35	1.0	10.52.30.36	6.1

Add Links

Available Links From 10.52.30.34

Link Name	From Ports	To Device	To Ports
	7.0	10.52.30.36	6.4
LINK-10.52.30.36-6.2--10.5...	1.0	10.52.30.36	6.2
	7.1	10.52.30.36	6.5

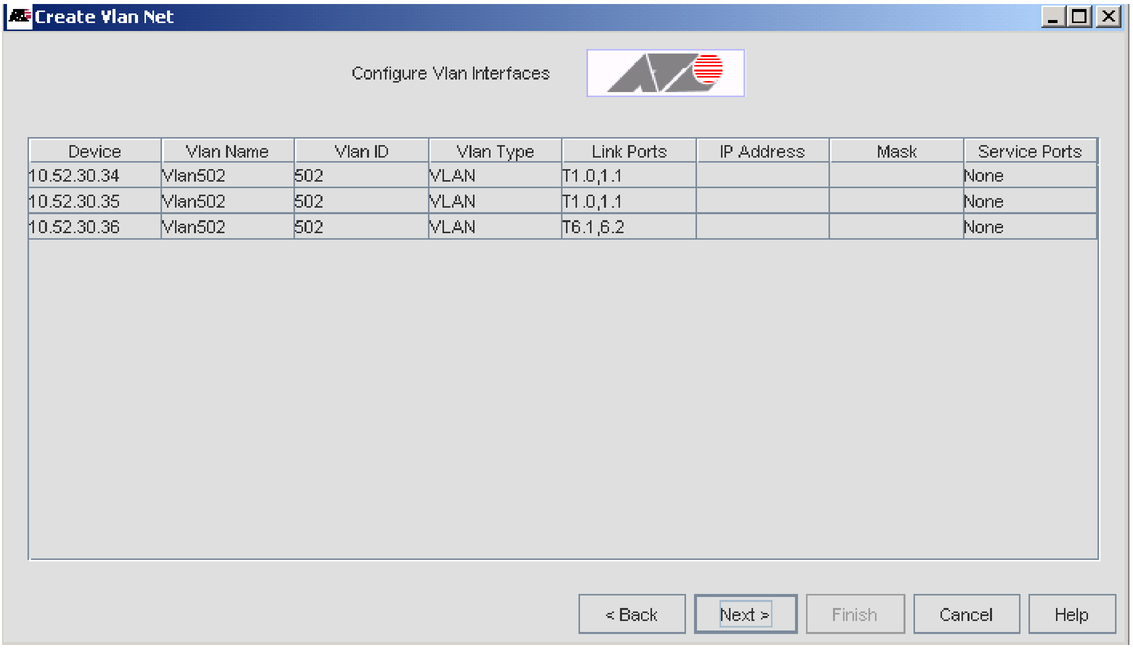
FIGURE 16-11 Adding Vlan Path Links - File

There is also the option to create a physical link by clicking **Create New Link**, and a new physical connection between two devices and their ports can be created. This uses the same form as shown in "Physical Network Map" on page 527.

16.3.3 Configure the VLAN Interfaces (Service Ports)

The next step is to configure the VLAN interfaces by adding any service ports to the Network VLAN. Service ports are those ports configured on the individual node and are the local VLAN interfaces. These ports can be configured as part of configuring VLAN ports for an individual device (as shown in Section "Configure VLAN (Chassis View)" on page 335), or they can be configured here.

When clicking **Next** in the **Modify Links** form, the **Configure VLAN Interfaces** form appears, as shown in Figure 16-12.



Create Vlan Net

Configure Vlan Interfaces

Device	Vlan Name	Vlan ID	Vlan Type	Link Ports	IP Address	Mask	Service Ports
10.52.30.34	Vlan502	502	VLAN	T1.0,1.1			None
10.52.30.35	Vlan502	502	VLAN	T1.0,1.1			None
10.52.30.36	Vlan502	502	VLAN	T6.1,6.2			None

FIGURE 16-12 Configure VLAN Interface Form - File

If this is an IP-based VLAN, you can enter the IP address in the cell in the **IpAddress** column, and the network mask in the cell in the **Mask** column. This must be extended to a specific address within the subnet. For the port row, click the IpAddress cell and enter the IP address, and then click the Mask cell and enter the network mask.

Note: If a VLAN subnet was entered on the first panel, when you click the IpAddress cell, the cell will be filled with the subnet address, and when you click the Mask cell for that row (or any other cell), the Mask cell will be filled with the mask value for the subnet. Typically, the Mask cell value will not need to be changed.

To configure service ports, click the **cell** in the **Service Ports** column and the **Edit Ports** form appears, as shown in Figure 16-13.

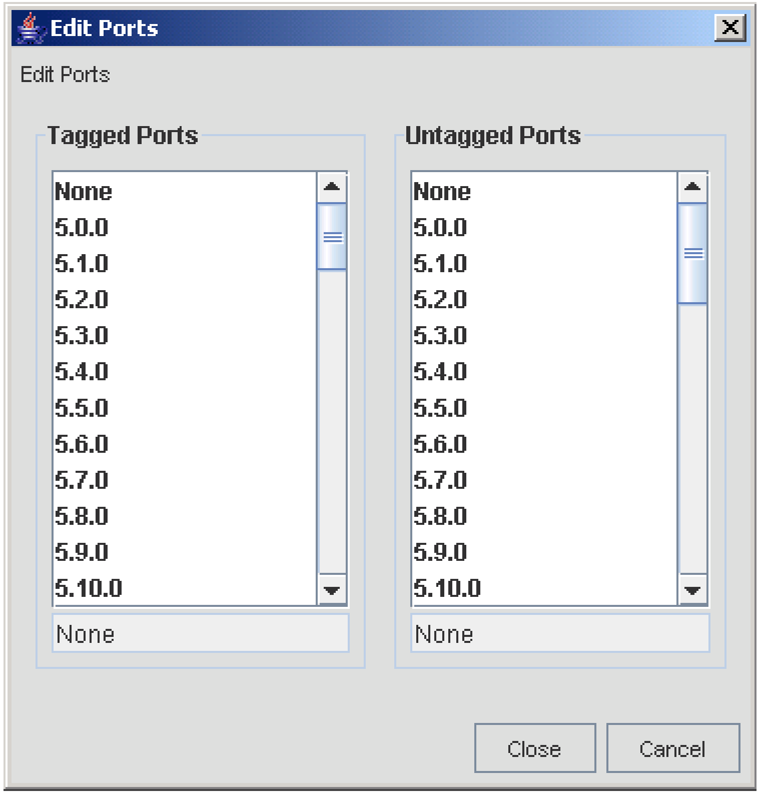
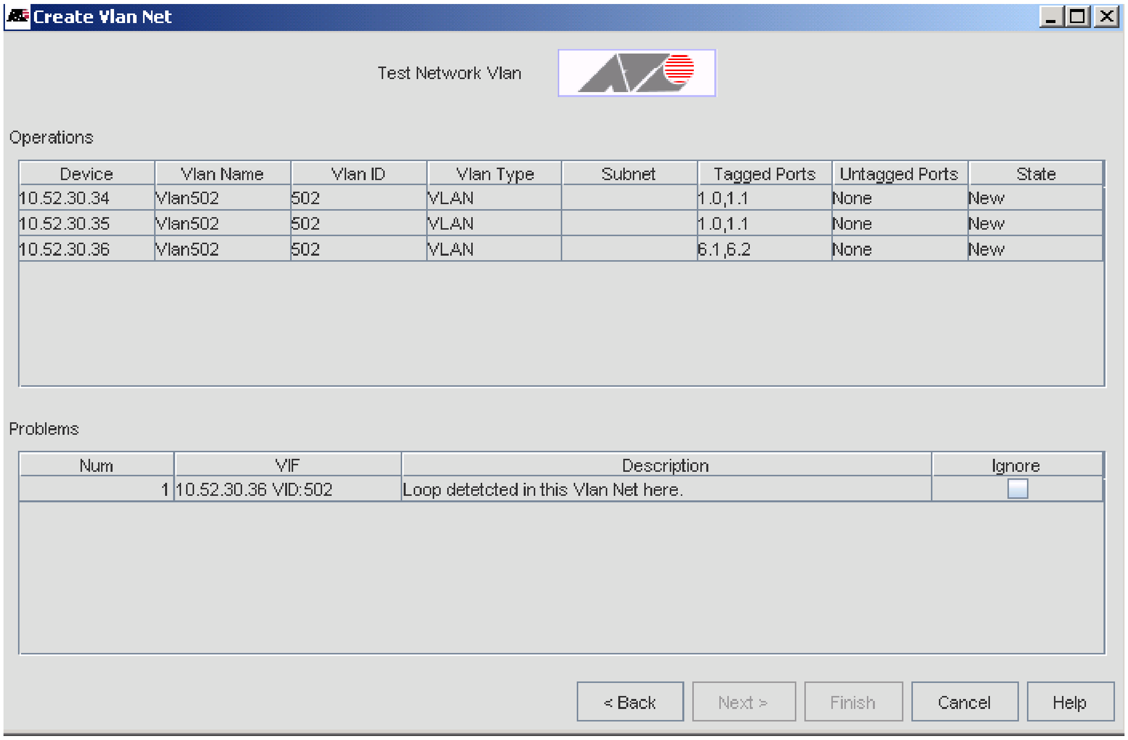


FIGURE 16-13 Edit Ports Form

Clicking on the ports and then clicking **Close** adds these to the Service Ports cell that was chosen. Multiple ports may be selected pressing the Shift or Ctrl key while clicking. The same port must not be selected in both the **Tagged Ports** and **Untagged Ports** lists. This error will be detected when the **Close** button is clicked. The form will not close until the error is corrected.

Once the VLAN Interfaces have been configured, clicking **Next** will invoke the **Test Network VLAN** form, which ensures that the Network VLAN has the ports configured correctly so that all ports can send data to all other ports within that Network VLAN. If there is a problem, a Problems table is added to the form, with a description, as shown in Figure 16-14. Some errors (warnings) can be ignored. In this case, the checkbox in the Ignore column can be checked and the Network VLAN will be created anyway. Other errors will prevent the VLAN from being created. These errors must be fixed by backing up to the previous panels and correcting the problem.



Device	Vlan Name	Vlan ID	Vlan Type	Subnet	Tagged Ports	Untagged Ports	State
10.52.30.34	Vlan502	502	VLAN		1.0,1.1	None	New
10.52.30.35	Vlan502	502	VLAN		1.0,1.1	None	New
10.52.30.36	Vlan502	502	VLAN		6.1,6.2	None	New

Num	VIF	Description	Ignore
1	10.52.30.36 VID:502	Loop detetcted in this Vlan Net here.	☐

FIGURE 16-14 Test Network VLAN Form (with error and option to ignore)

16.4 Extending Network VLANs

Once a Network VLAN is created, the general procedure for extending it is as follows:

1. Open the Network VLAN submap associated with the VLAN. This can be done by right-clicking the desired VLAN on the main Network VLAN map and selecting *Open Submap* from the pop-up menu.
2. In the VLAN submap, right-click the VLAN IF from which you want to extend the VLAN, and then select *Extend Vlan* from the pop-up menu. The **Extend Network Vlan** form will appear.

Note: You can also extend a VLAN from a particular VLAN IF by right-clicking the VLAN IF in the VLAN Interfaces table, and then selecting Extend Vlan from the pop-up menu.

3. Select or create a link over which to extend the VLAN.
4. Create/select a new VLAN IF on the device at the other end of the selected link. This new VLAN IF will become part of the network VLAN.

The concept behind this procedure is shown in the following figure.

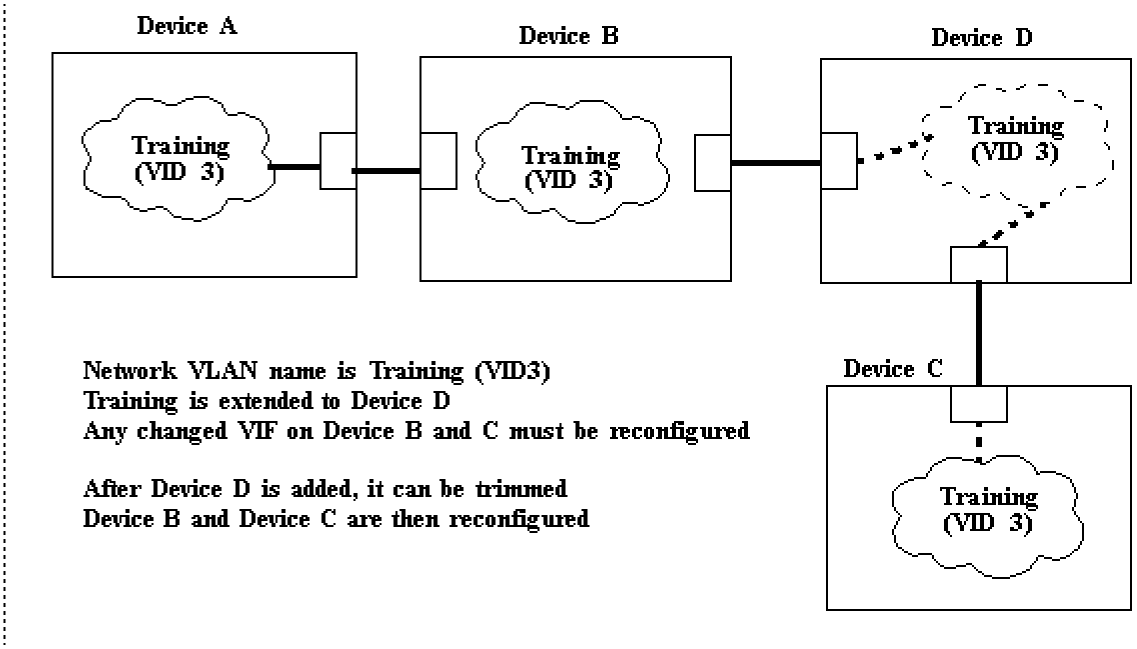
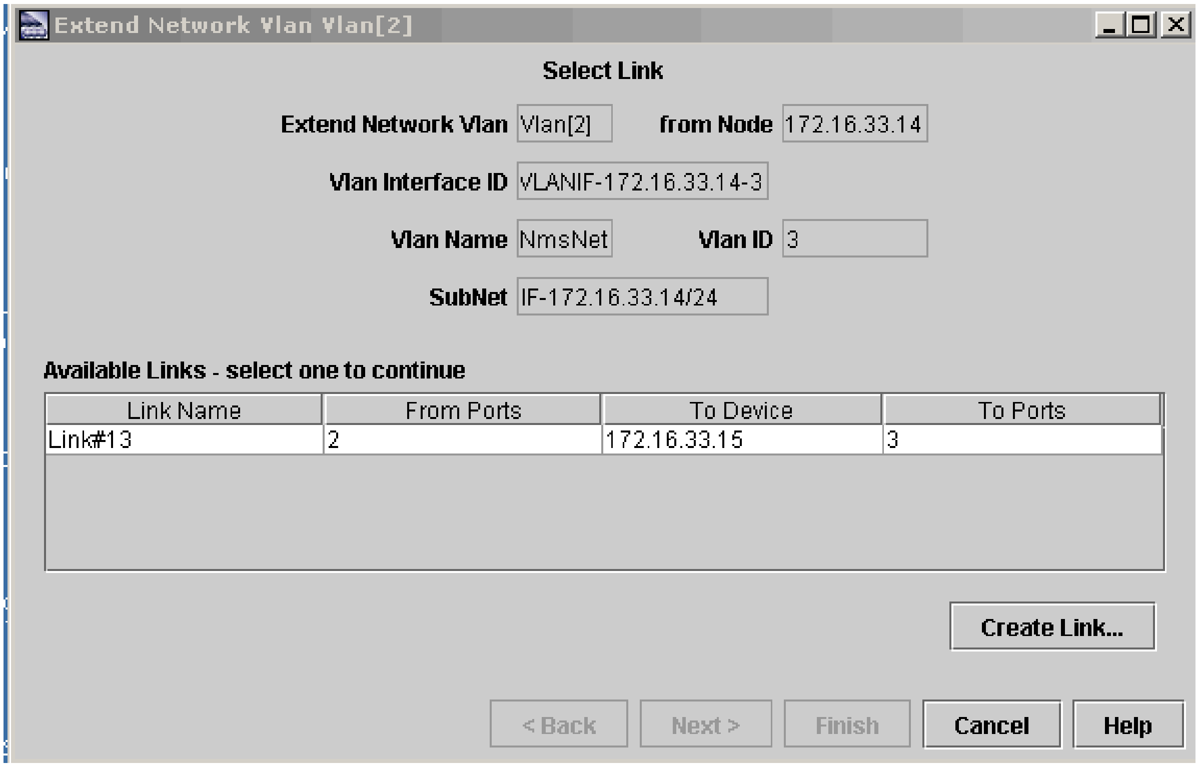

Device A
Training (VID 3)
Device B
Training (VID 3)
Device D
Training (VID 3)
Device C
Training (VID 3)
Network VLAN name is Training (VID3)
Training is extended to Device D
Any changed VIF on Device B and C must be reconfigured
After Device D is added, it can be trimmed
Device B and Device C are then reconfigured

FIGURE 16-15 Extending a Network VLAN

The **Extend Network VLAN** form that appears when you select *Extend Vlan* from the pop-up menu is shown in Figure 16-16.



Extend Network Vlan: Vlan[2]
from Node: 172.16.33.14
Vlan Interface ID: VLANIF-172.16.33.14-3
Vlan Name: NmsNet
Vlan ID: 3
SubNet: IF-172.16.33.14/24

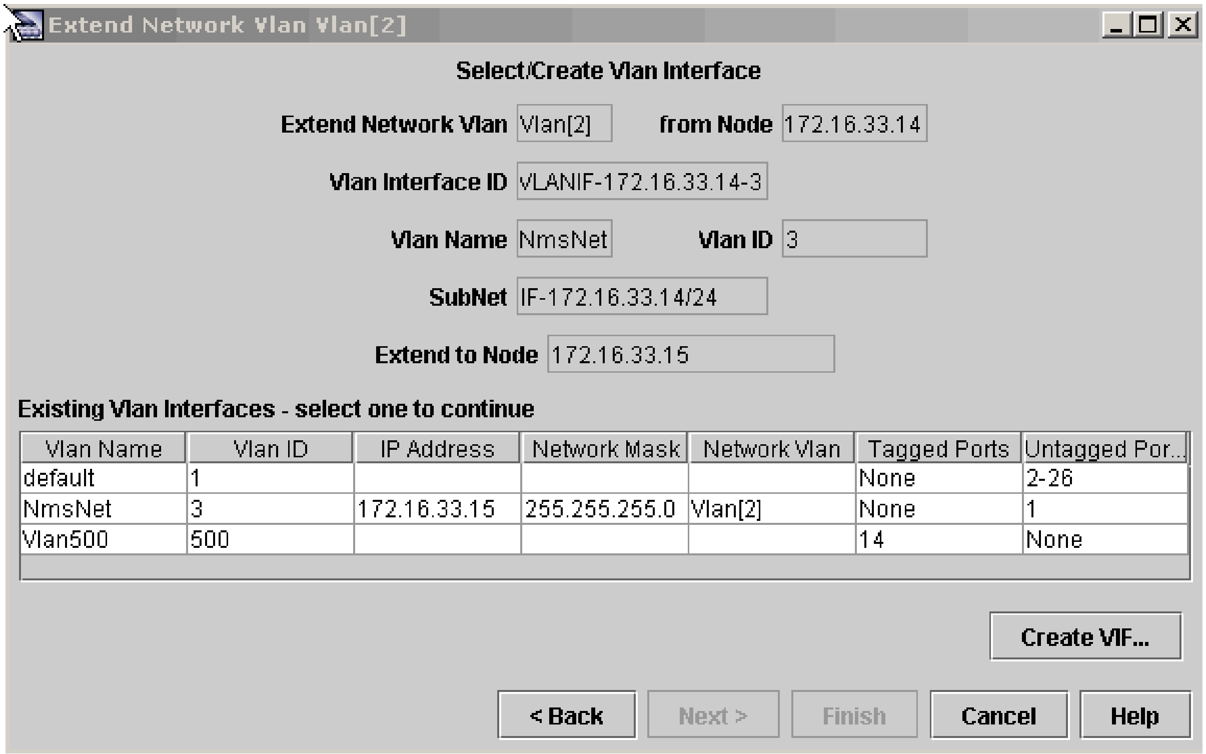
Available Links - select one to continue

Link Name	From Ports	To Device	To Ports
Link#13	2	172.16.33.15	3

FIGURE 16-16 Extend Network VLAN Form (Physical Link)

This form shows Network VLAN Name, the VLAN ID (VID), and the available links from the device selected. (At this point a new physical link can be created between this device and the device that will include the Network VLAN. Refer to "Physical Network Map" on page 527.)

Select **one** of the available physical links to activate the **Next** button. The form that shows the available VLAN IFs on this physical link is displayed, as shown in Figure 16-17.



Select/Create Vlan Interface

Extend Network Vlan Vlan[2] from Node 172.16.33.14

Vlan Interface ID VLANIF-172.16.33.14-3

Vlan Name NmsNet Vlan ID 3

SubNet IF-172.16.33.14/24

Extend to Node 172.16.33.15

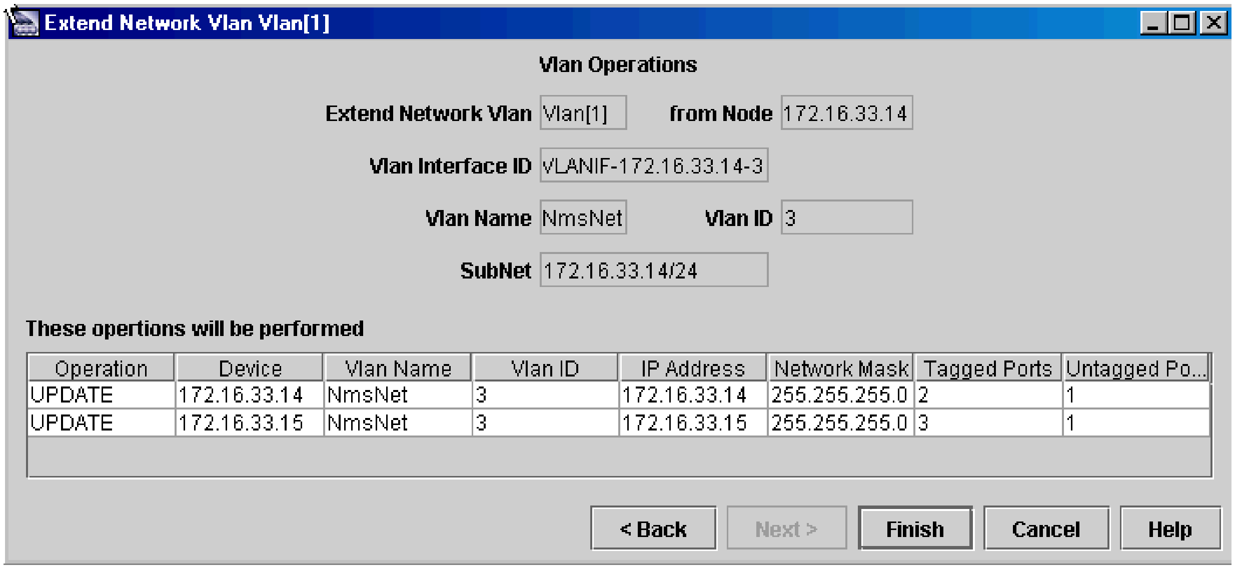
Existing Vlan Interfaces - select one to continue

Vlan Name	Vlan ID	IP Address	Network Mask	Network Vlan	Tagged Ports	Untagged Por...
default	1				None	2-26
NmsNet	3	172.16.33.15	255.255.255.0	Vlan[2]	None	1
Vlan500	500				14	None

FIGURE 16-17 Extend Network VLAN Form (VLAN Interface) - File

Select one of the VLAN Interfaces. (At this point a new VLAN Interface can be created on the device.)

Select **one** of the available VLAN Interfaces to activate the **Next** button. The form that summarizes how the VLAN Network will be extended is displayed, as shown in Figure 16-18.



Vlan Operations

Extend Network Vlan Vlan[1] from Node 172.16.33.14

Vlan Interface ID VLANIF-172.16.33.14-3

Vlan Name NmsNet Vlan ID 3

SubNet 172.16.33.14/24

These opertions will be performed

Operation	Device	Vlan Name	Vlan ID	IP Address	Network Mask	Tagged Ports	Untagged Po...
UPDATE	172.16.33.14	NmsNet	3	172.16.33.14	255.255.255.0	2	1
UPDATE	172.16.33.15	NmsNet	3	172.16.33.15	255.255.255.0	3	1

FIGURE 16-18 Extend Network VLAN Form - Finish

The IP address and network mask can be entered in cells **IP Address** and **Network Mask** respectively by clicking the cell and entering the value.

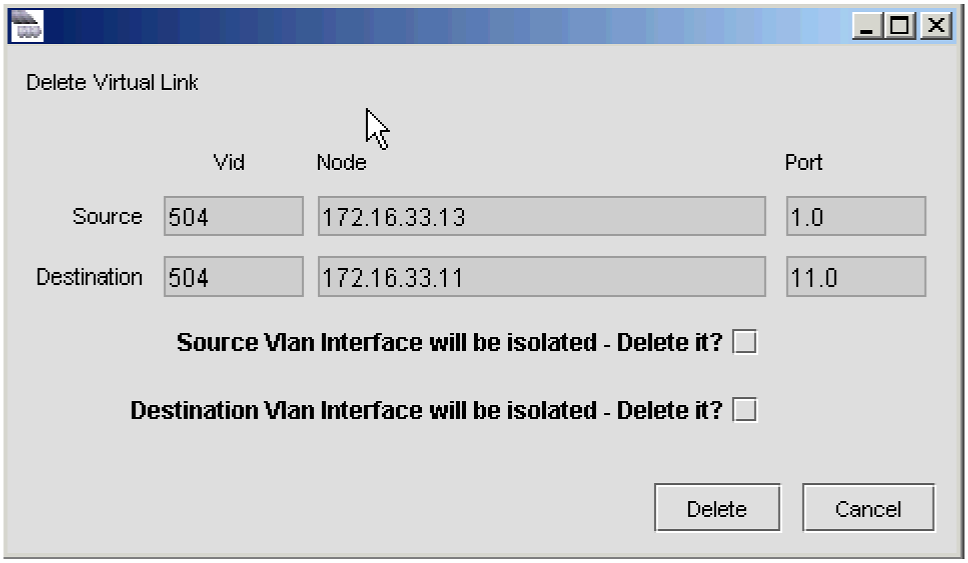
Note: *When you click the IP Address cell, the cell will be filled with the subnet address, and when you click the Network Mask cell (or any other cell), the cell will be filled with the network mask for the subnet.*

Clicking **Finish** button will invoke the **Task Details** form and list the subtasks to be done. The Task Status field gives the state of the task, and if the Execution state is Failed, double-clicking the row will display the reasons for the failure in an Error Details pop-up.

16.5 Trimming or Splitting Network VLANs

A network VLAN can be trimmed or split as follows:

1. Open the submap for the VLAN and locate the link to be removed.
2. Right-click the link to be removed, and then select *Delete Vlan Link* from the pop-up menu. The dialog box shown in the following figure will appear. The dialog box shows the VID, node, and port that will be removed.



Delete Virtual Link

	Vid	Node	Port
Source	504	172.16.33.13	1.0
Destination	504	172.16.33.11	11.0

Source Vlan Interface will be isolated - Delete it? □

Destination Vlan Interface will be isolated - Delete it? □

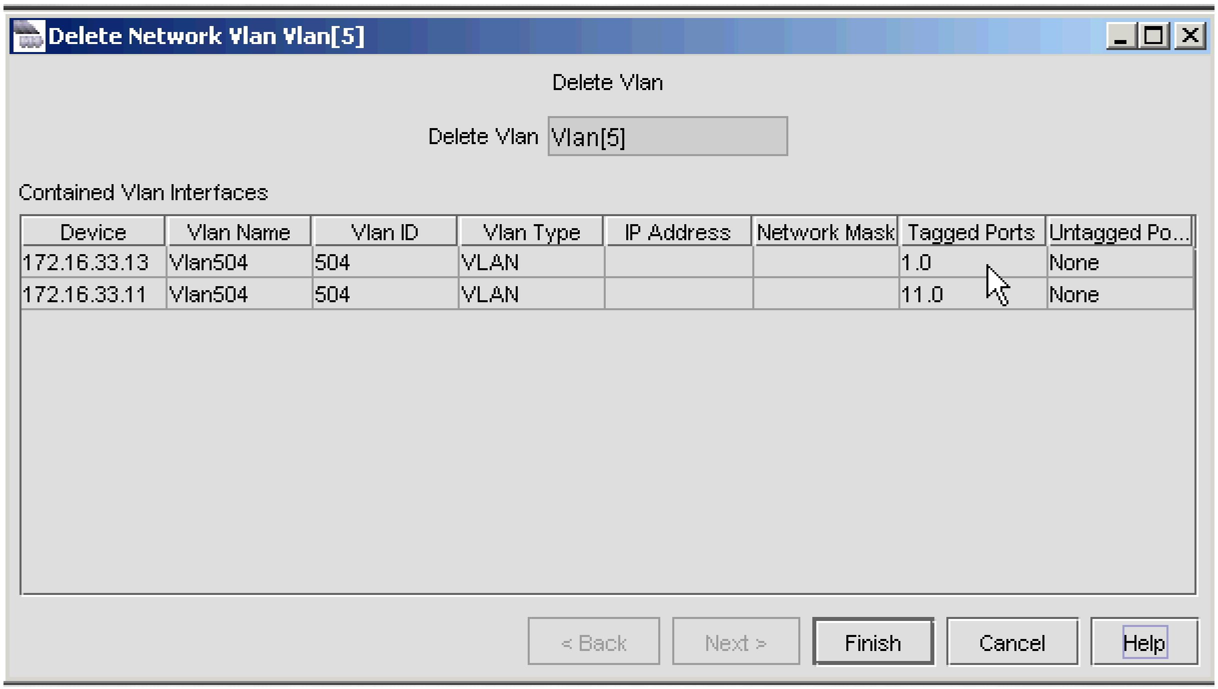
FIGURE 16-19 Delete Virtual Link Dialog Box

3. If the **Source Vlan Interface will be isolated - Delete it?** checkbox appears (as shown in Figure 16-19), checking this box will cause the source VLAN IF to be removed. If you want to remove the VLAN IF, check this box.
4. If the **Destination Vlan Interface will be isolated - Delete it?** checkbox appears, checking this box will cause the destination VLAN IF to be removed. If you want to remove the VLAN IF, check this box.
5. Click **Delete**. The View Task Details dialog box will appear.

16.6 Deleting Network VLANs

Deleting a Network VLAN can be done in the Physical Network or Network VLAN map. In the Physical Network map, select the **Network Services** pull-down, and then select *VLAN -> Delete VLAN*. In the Network VLAN map, select *VLAN Operations -> Delete VLAN.*

In either case, all available Network VLANs appear in the Delete Network VLAN form, as shown in Figure 16-20.



Delete Vlan: Vlan[5]

Contained Vlan Interfaces

Device	Vlan Name	Vlan ID	Vlan Type	IP Address	Network Mask	Tagged Ports	Untagged Po...
172.16.33.13	Vlan504	504	VLAN			1.0	None
172.16.33.11	Vlan504	504	VLAN			11.0	None

FIGURE 16-20 Delete Network VLANs Form

Select one of the VLAN IDs, and then click **Delete VLAN**. A form showing all the associated VLAN Interfaces that will also be deleted will appear. If this is what you wish to do, click **Finish**. The Task Details window then will appear.

Note: *VLAN Interfaces with VID of 1, the default VLAN, will not be deleted.*

16.7 Network VLAN Manager (Excluding EPSR)

16.7.1 Overview

The Network VLAN Manager/Analyzer includes the following functions:

- Shows in a hierarchy all the Network VLANs and their associated VLAN Interfaces.
- Shows in a hierarchy all the Device VLANs.
- Imports a spreadsheet of physical link attributes that automatically provisions the links and creates any associated Network VLANs.
- Displays VLAN outage statistics.
- Provides Port Management

Following is a description of these functions

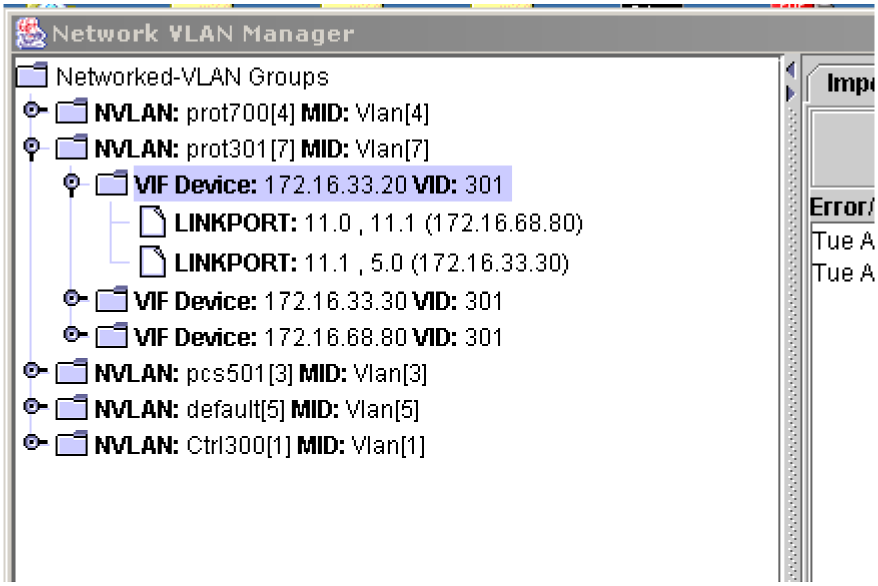
Note: *The functions of the Network VLAN Manager include all aspects of VLAN management, including configuring VLANs for Ethernet Protection Switching RIng (EPSR). All of these capabilities are explained here, with the exception of EPSR, which is explained in "Protection Switching-EPSR" on page 567.*

16.7.2 Create Network VLAN

When viewing the network VLANs, the user can select and then right-click the top node (Networked-VLAN Groups) and select Create New Networked VLAN. This is the same form as Figure 16-9.

16.7.3 Using the Network VLAN Hierarchy

Viewing the Network VLAN Manager/Analyzer is done from the Physical Network map. From the Network Service menu, select *VLAN -> Network VLAN Manager*. The **Network VLAN Manager/Analyzer** form appears, as shown in the following figure. The **View Networked VLANs** view is selected.



Network VLAN Manager

Networked-VLAN Groups
- **NVLAN:** prot700[4] **MID:** Vlan[4]
- **NVLAN:** prot301[7] **MID:** Vlan[7]
  - **VIF Device:** 172.16.33.20 **VID:** 301
    - **LINKPORT:** 11.0 , 11.1 (172.16.68.80)
    - **LINKPORT:** 11.1 , 5.0 (172.16.33.30)
  - **VIF Device:** 172.16.33.30 **VID:** 301
  - **VIF Device:** 172.16.68.80 **VID:** 301
- **NVLAN:** pcs501[3] **MID:** Vlan[3]
- **NVLAN:** default[5] **MID:** Vlan[5]
- **NVLAN:** Ctrl300[1] **MID:** Vlan[1]

FIGURE 16-21 Network VLAN Manager/Analyzer Panel (Network VLAN Hierarchy)

All available Network VLANs are shown in a hierarchy.

Selecting and right clicking on the Network VLAN, VLAN Interface Device, or LINKPORT Node node allows the administrator to perform various tasks, listed in the following table.

TABLE 16-5 Network VLAN Functions on the Network VLAN Manager

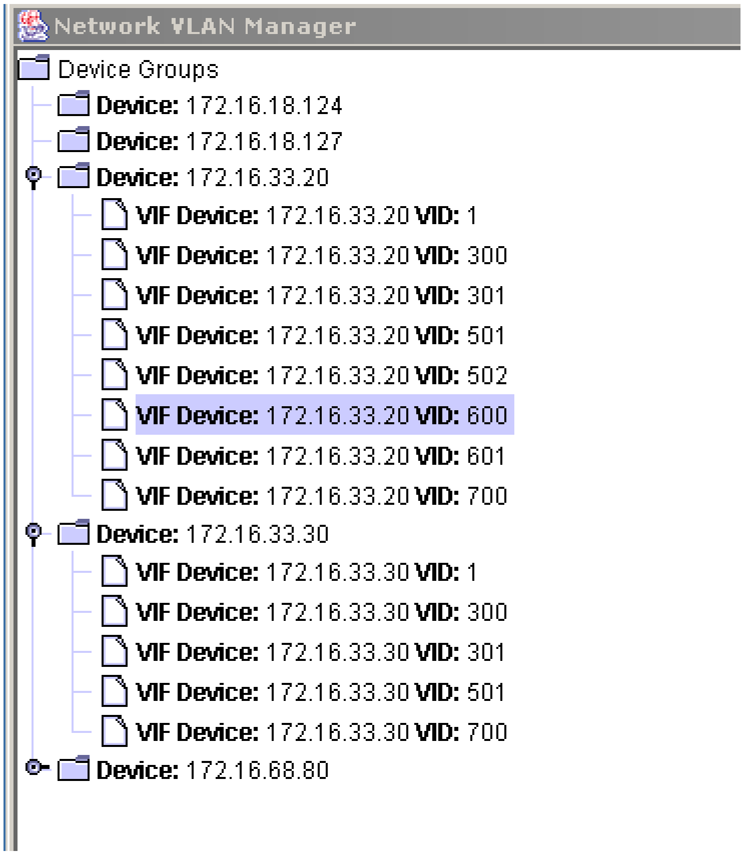
Type of VLAN	Function	Description
Networked VLANs	Show Map...	Show the logical map for the network VLAN as a layered window in the NMS application.
	Show Detach Map...	Show a detached map, allowing it to be moved outside the NMS work area and closed separately.
	Delete Networked VLAN...	Brings up the Delete Networked VLAN form, the same as in "Deleting Network VLANs" on page 542.
	Resync VIFs with Device...	Query and re synchronize the VLANs and their associated ports on all the relevant devices
VIF Device	View VLAN Interface...	Brings up chassis view for the VLAN Interface chosen
	Extend VLAN...	Extends the chosen VLAN. Refer to "Extending Network VLANs" on page 539
	Resync Device...	Query and re synchronize the VLANs and their associated ports on the selected device

TABLE 16-5 Network VLAN Functions on the Network VLAN Manager

Type of VLAN	Function	Description
LINKPORT	View Link Port	Brings up the Port Management Form.
	View Neighbor Link Port...	Brings up the port management form for the next port in the VLAN hierarchy in the left panel.
	Delete Logical Link	Brings up the Delete Virtual Link form, which deletes the VLAN path between two devices (not the physical link).
	Delete Assoc. Physical Link...	Deletes the physical link associated with the logical link. Note that if there are other logical links on the virtual link, the screen will not appear.

16.7.4 Using the Device VLAN Hierarchy

Selecting **View Device VLANs** in the lower right of the Network VLAN Manager brings up the Device hierarchy, as shown in the following figure:


Network VLAN Manager

Device Groups

- **Device:** 172.16.18.124
- **Device:** 172.16.18.127
- **Device:** 172.16.33.20
  - **VIF Device:** 172.16.33.20 **VID:** 1
  - **VIF Device:** 172.16.33.20 **VID:** 300
  - **VIF Device:** 172.16.33.20 **VID:** 301
  - **VIF Device:** 172.16.33.20 **VID:** 501
  - **VIF Device:** 172.16.33.20 **VID:** 502
  - **VIF Device:** 172.16.33.20 **VID:** 600
  - **VIF Device:** 172.16.33.20 **VID:** 601
  - **VIF Device:** 172.16.33.20 **VID:** 700
- **Device:** 172.16.33.30
  - **VIF Device:** 172.16.33.30 **VID:** 1
  - **VIF Device:** 172.16.33.30 **VID:** 300
  - **VIF Device:** 172.16.33.30 **VID:** 301
  - **VIF Device:** 172.16.33.30 **VID:** 501
  - **VIF Device:** 172.16.33.30 **VID:** 700
- **Device:** 172.16.68.80

FIGURE 16-22 Network VLAN Manager (Device VLAN Hierarchy)

Right clicking on the Network VLAN, VIF Device, or LINKPORT Node node allows the administrator to perform various tasks, listed in the following table

TABLE 16-6 Device VLAN Functions on the Network VLAN Manager

Type of VLAN	Function	Description
VLAN Interface (VIF) Device	View VLAN Interface...	Brings up chassis view for the VLAN Interface chosen
	Extend VLAN...	Extends the chosen VLAN. Refer to "Extending Network VLANs" on page 539
	Resync Device...	Query and re synchronize the VLANs and their associated ports on the selected device.

Note: The last selection, View Protection Domains, is covered in the EPSR subsection, "Protection Switching-EPSR" on page 567.

16.7.5 Importing Physical Link Configurations

Since the physical link configuration for an existing network can be large and complex, the Network VLAN Manager can have an Excel spreadsheet of the physical links imported. This will populate the Physical Network map, and any existing Network VLANs that use those links will be configured.

Following are the rules for creating the link configuration file for this release:

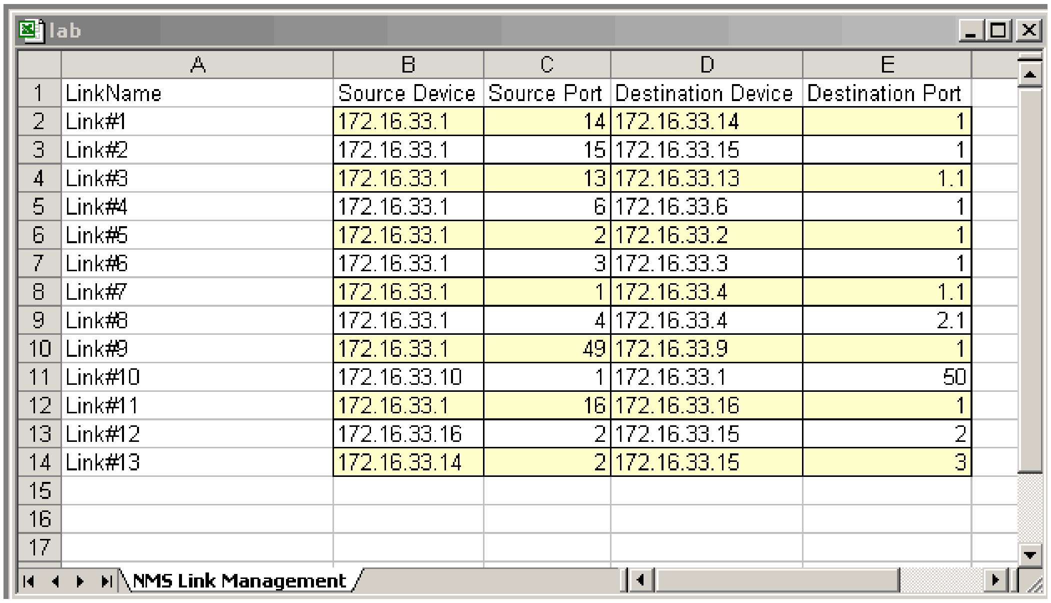
- The file must be an Excel spreadsheet. (Future releases will support other filetypes.)

Note: When the AlliedView NMS is on a Sun platform, an Excel spreadsheet can still be imported, although it cannot be viewed by the user.

- The heading row must have the following columns:
  - **LinkName** - The name of the link (values are optional)
  - **Source Device** - A known device that the AlliedView NMS will have already discovered
  - **Source Port** - A valid port on the source device
  - **Destination Device** - A known device that the AlliedView NMS will have already discovered
  - **Destination Port** - A valid port on the desalination device
- The spreadsheet must reside in the following directory on the NMS:

```
<server path>\Allied Telesis\AlliedViewNMS\<NMS load>\state
```

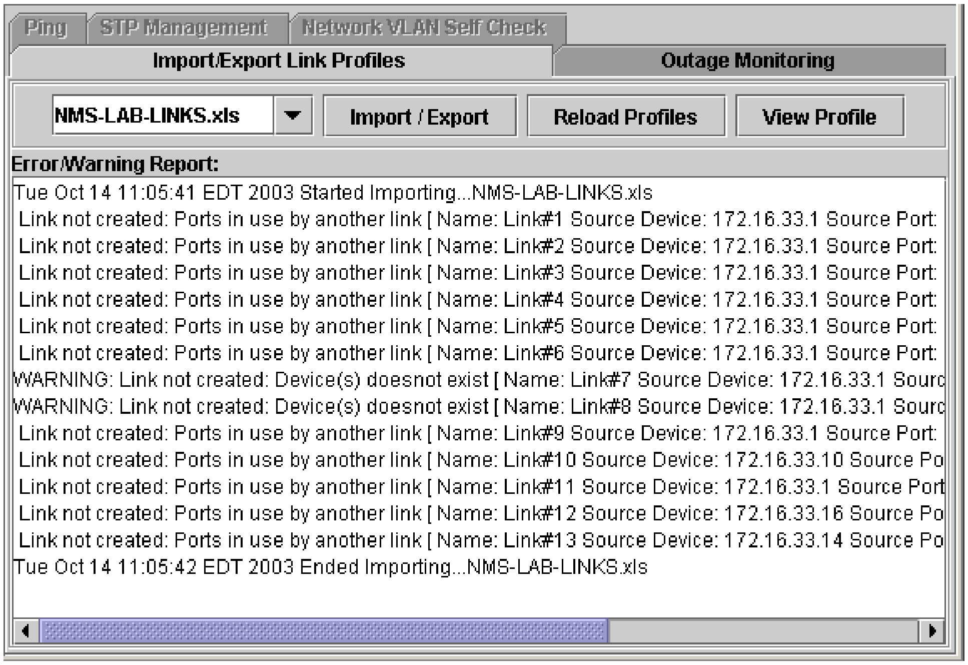
Figure 16-23 shows an example of spreadsheet in Microsoft Excel.



	A	B	C	D	E
1	LinkName	Source Device	Source Port	Destination Device	Destination Port
2	Link#1	172.16.33.1	14	172.16.33.14	1
3	Link#2	172.16.33.1	15	172.16.33.15	1
4	Link#3	172.16.33.1	13	172.16.33.13	1.1
5	Link#4	172.16.33.1	6	172.16.33.6	1
6	Link#5	172.16.33.1	2	172.16.33.2	1
7	Link#6	172.16.33.1	3	172.16.33.3	1
8	Link#7	172.16.33.1	1	172.16.33.4	1.1
9	Link#8	172.16.33.1	4	172.16.33.4	2.1
10	Link#9	172.16.33.1	49	172.16.33.9	1
11	Link#10	172.16.33.10	1	172.16.33.1	50
12	Link#11	172.16.33.1	16	172.16.33.16	1
13	Link#12	172.16.33.16	2	172.16.33.15	2
14	Link#13	172.16.33.14	2	172.16.33.15	3
15					
16					
17					

FIGURE 16-23 Example Physical Link Spreadsheet

To ensure that all files in the state directory are available, select Reload Profiles. To actually import the spreadsheet, select Import/Export. As the links are loaded, progress messages will appear, as shown in Figure 16-24.



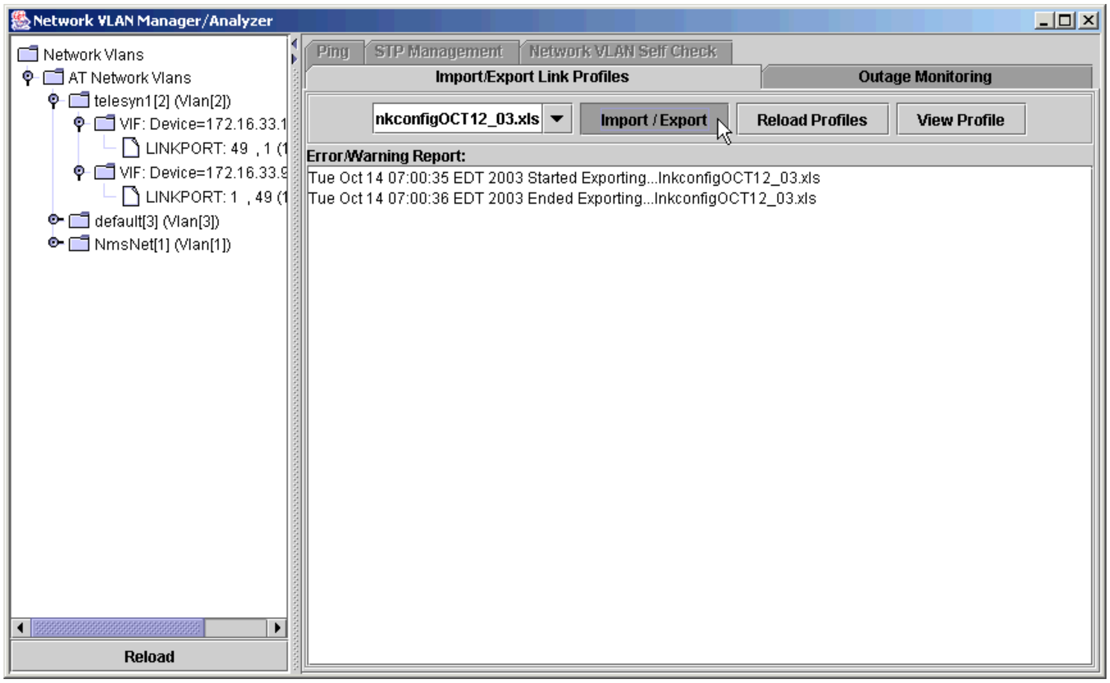
```
Tue Oct 14 11:05:41 EDT 2003 Started Importing...NMS-LAB-LINKS.xls
 Link not created: Ports in use by another link [ Name: Link#1 Source Device: 172.16.33.1 Source Port:
 Link not created: Ports in use by another link [ Name: Link#2 Source Device: 172.16.33.1 Source Port:
 Link not created: Ports in use by another link [ Name: Link#3 Source Device: 172.16.33.1 Source Port:
 Link not created: Ports in use by another link [ Name: Link#4 Source Device: 172.16.33.1 Source Port:
 Link not created: Ports in use by another link [ Name: Link#5 Source Device: 172.16.33.1 Source Port:
 Link not created: Ports in use by another link [ Name: Link#6 Source Device: 172.16.33.1 Source Port:
WARNING: Link not created: Device(s) doesnot exist [ Name: Link#7 Source Device: 172.16.33.1 Sourc
WARNING: Link not created: Device(s) doesnot exist [ Name: Link#8 Source Device: 172.16.33.1 Sourc
 Link not created: Ports in use by another link [ Name: Link#9 Source Device: 172.16.33.1 Source Port:
 Link not created: Ports in use by another link [ Name: Link#10 Source Device: 172.16.33.10 Source Po
 Link not created: Ports in use by another link [ Name: Link#11 Source Device: 172.16.33.1 Source Port
 Link not created: Ports in use by another link [ Name: Link#12 Source Device: 172.16.33.16 Source Po
 Link not created: Ports in use by another link [ Name: Link#13 Source Device: 172.16.33.14 Source Po
Tue Oct 14 11:05:42 EDT 2003 Ended Importing...NMS-LAB-LINKS.xls
```

FIGURE 16-24 Error Messages When Importing Physical Links

Figure 16-24 shows an example of error messages, when the spreadsheet contains links that already physically exist.

16.7.6 Exporting Physical Link Configurations

The physical link configuration can be exported to an Excel file as well. If the user provides a file name that ends with **.xls** and if that file name is not associated with an existing profile, the AlliedView NMS will export the current NMS physical link data to the specified Excel file. This is shown in the following figure.



```
Tue Oct 14 07:00:35 EDT 2003 Started Exporting...lnkconfigOCT12_03.xls
Tue Oct 14 07:00:36 EDT 2003 Ended Exporting...lnkconfigOCT12_03.xls
```

FIGURE 16-25 Exporting Link Configuration Data to an Excel File

If the user selects an existing profile or specifies the name of an existing profile, the data will be imported from the specified Excel file and not re-exported. Any existing links included in the file will be skipped.

16.7.7 Viewing VLAN Outage Statistics

The VLAN Outage Monitor provides long-term outage statistics on individual VLANs, which allows you to determine how your VLANs are performing over time. The VLAN Outage Monitor uses the Link Down trap to determine when an outage has occurred and the Link Up trap to determine when the outage is cleared. The statistics recorded by the VLAN Outage Monitor are stored in the NMS database and include:

- Network VLAN name – Name of the monitored Network VLAN
- Availability - The availability of the VLAN expressed as a value from 0 to 1 (0 percent availability to 100 percent availability)
- Outage Time – Approximate total outage time in days, hours, minutes, seconds, and milliseconds
- MTTR - Approximate mean time to repair in hours calculated as Total Down Time / Number of Failures
- MTBF - Approximate mean time between failures in hours calculated as Total Up Time / Number of Failures
- Number of Failures – Number of failures recorded
- Start Monitor Time – This is the time when the Network VLAN was first created or the last time when the monitoring was reset.
- Duration – The approximate elapsed time in hours between the Start Monitor Time and Current Monitor Time

The following figure demonstrates a typical monitoring timeline.

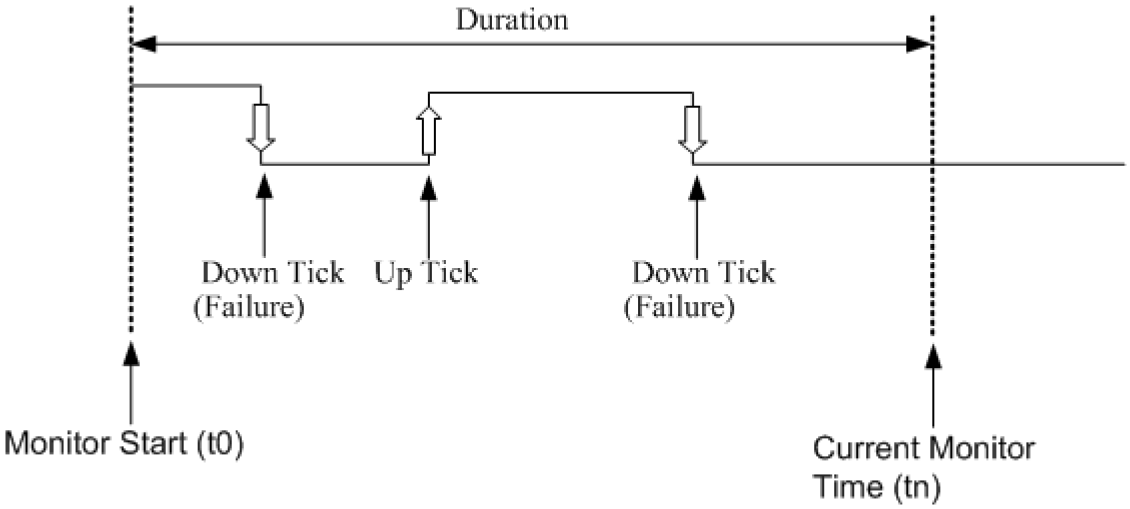


FIGURE 16-26 Sample VLAN Outage Monitoring Timeline

Note: For protection schemes, such as EPSR, when there is a break in the network VLAN topology due to link failure, an alternate path allows traffic to continue to run. As a result, these will not be recorded as outages and therefore will not appear for that networked VLAN. For more detail on EPSR, refer to "Protection Switching-EPSR" on page 567.

The Outage Monitoring tab of the VLAN Manager is shown in the following figure.

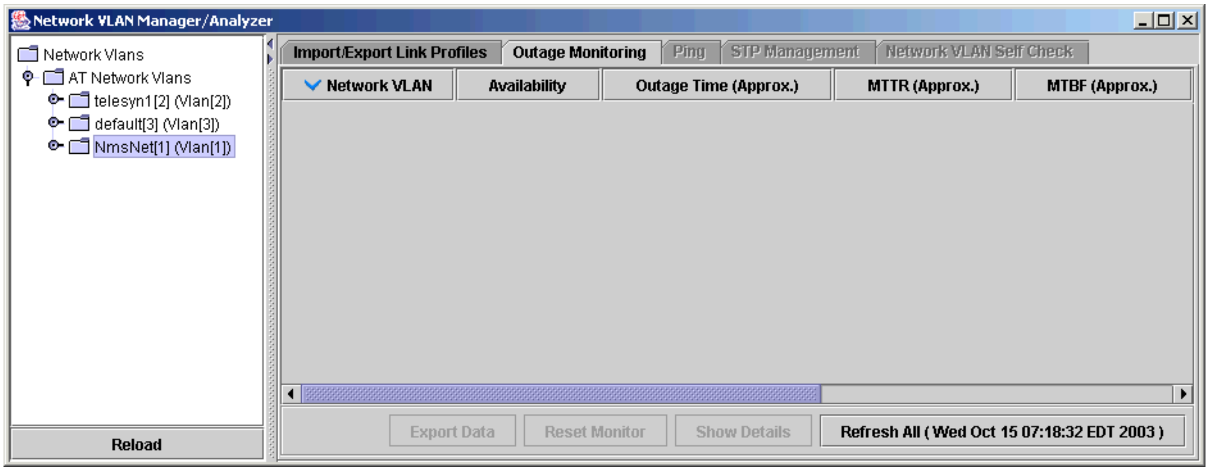


FIGURE 16-27 VLAN Manager Outage Monitoring Tab

16.7.7.1 Viewing Details

To see the VLAN outage details, select a VLAN in the list, and then click **Show Details**. The Network Vlan Outage Details window, shown in the following figure, is displayed.

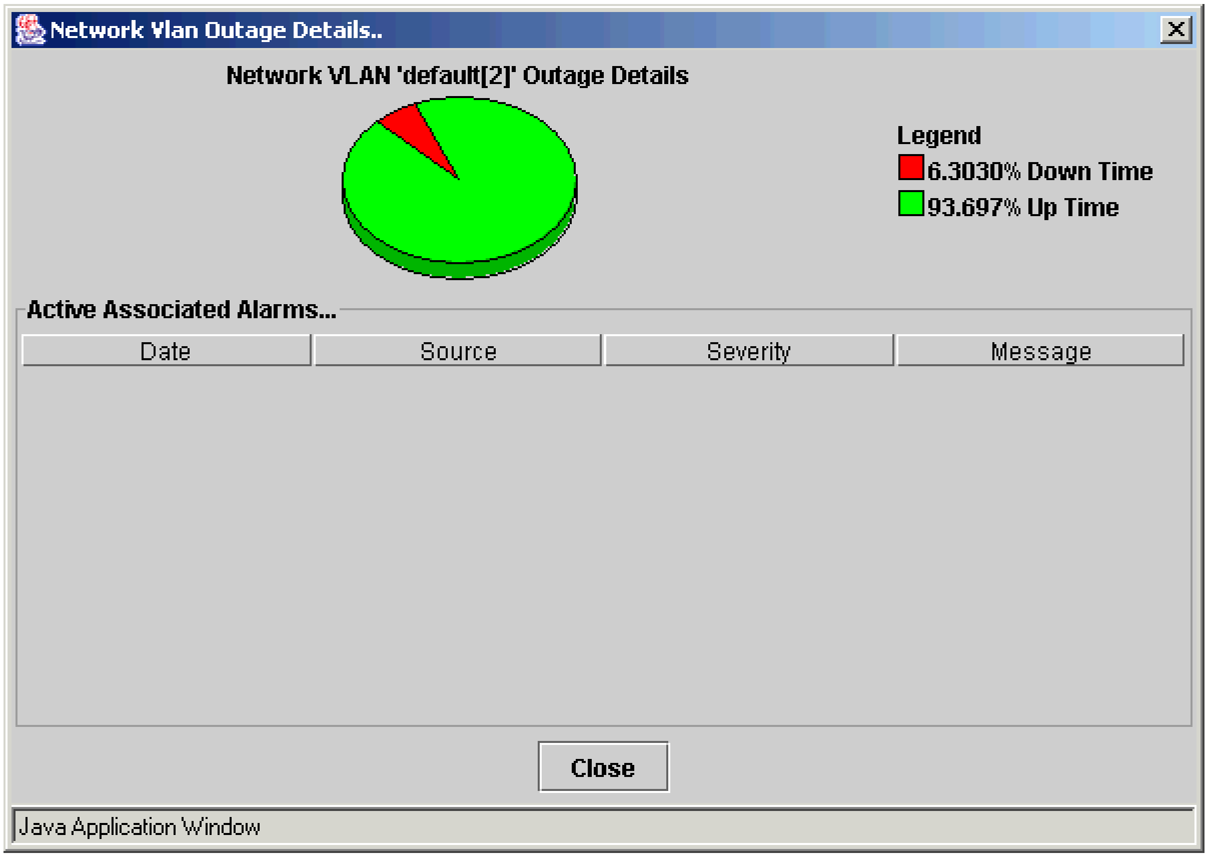

Network Vlan Outage Details..
Network VLAN 'default[2]' Outage Details
Legend
🟥6.3030% Down Time
🟩93.697% Up Time
Active Associated Alarms...
Date
Source
Severity
Message
Close
Java Application Window

FIGURE 16-28 Network Vlan Outage Details Window

16.7.7.2 Resetting Monitor Time

To reset the monitor time (i.e. set the monitor start time to the current monitor time), select a VLAN from the list, and then click **Reset Monitor**.

16.7.7.3 Refreshing all Network VLANs

To refresh all of the VLANs in the list, click **Refresh All**.

16.7.7.4 Exporting Outage Data

To export outage data to a file, select the records you wish to export, and then click **Export Data**. Specify the destination as a file or a printer.

16.8 Example of Creating Network VLANs

To show how all of these maps and forms work together when creating a Network VLAN, a sample IP-based and a sample island-based Network VLAN are created in this subsection.

16.8.1 Sample Island-Based Network VLAN

Figure 16-29 includes an iMAP 9400, an iMAP 9700, and a Rapier 48i. The values seen in this figure will be reflected in the sample steps.

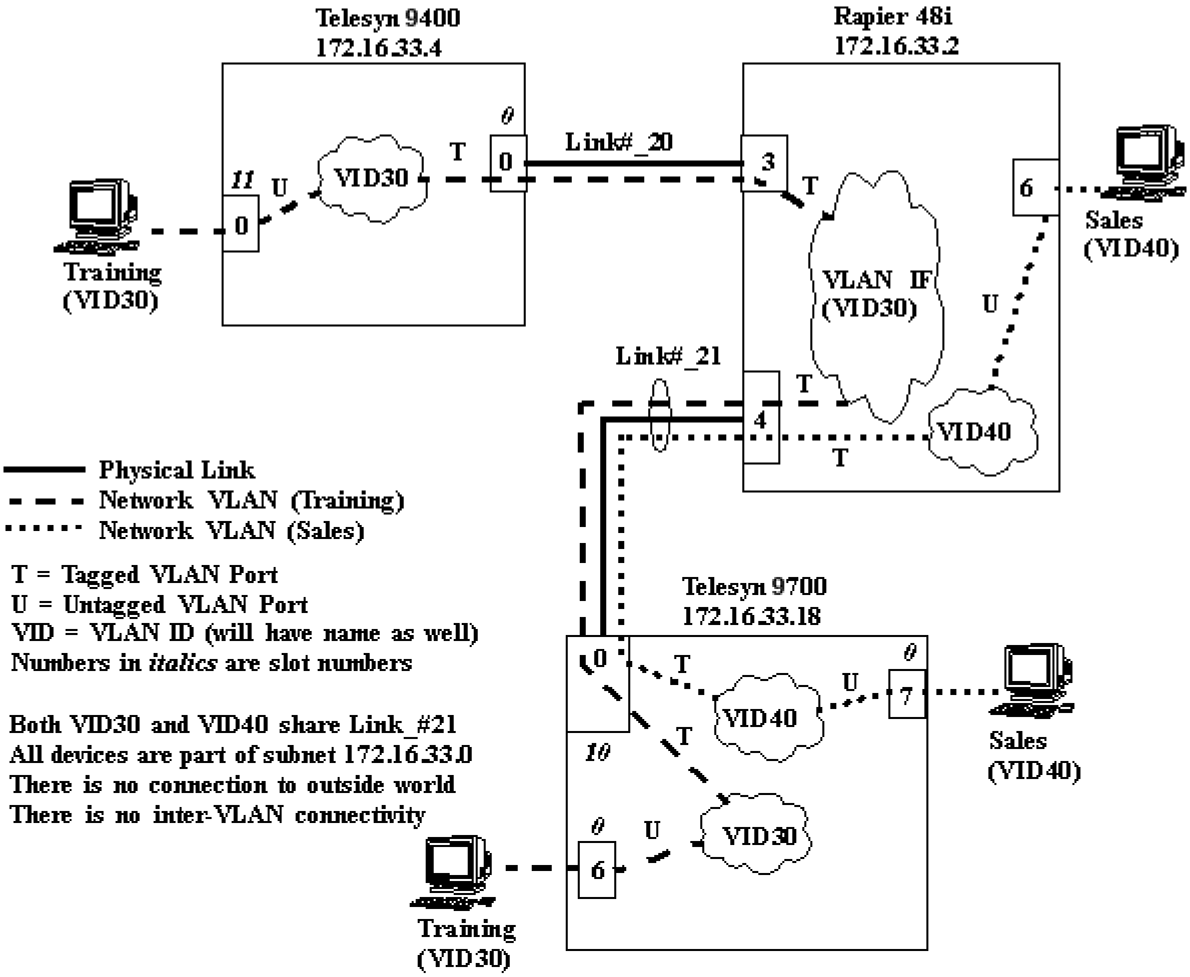
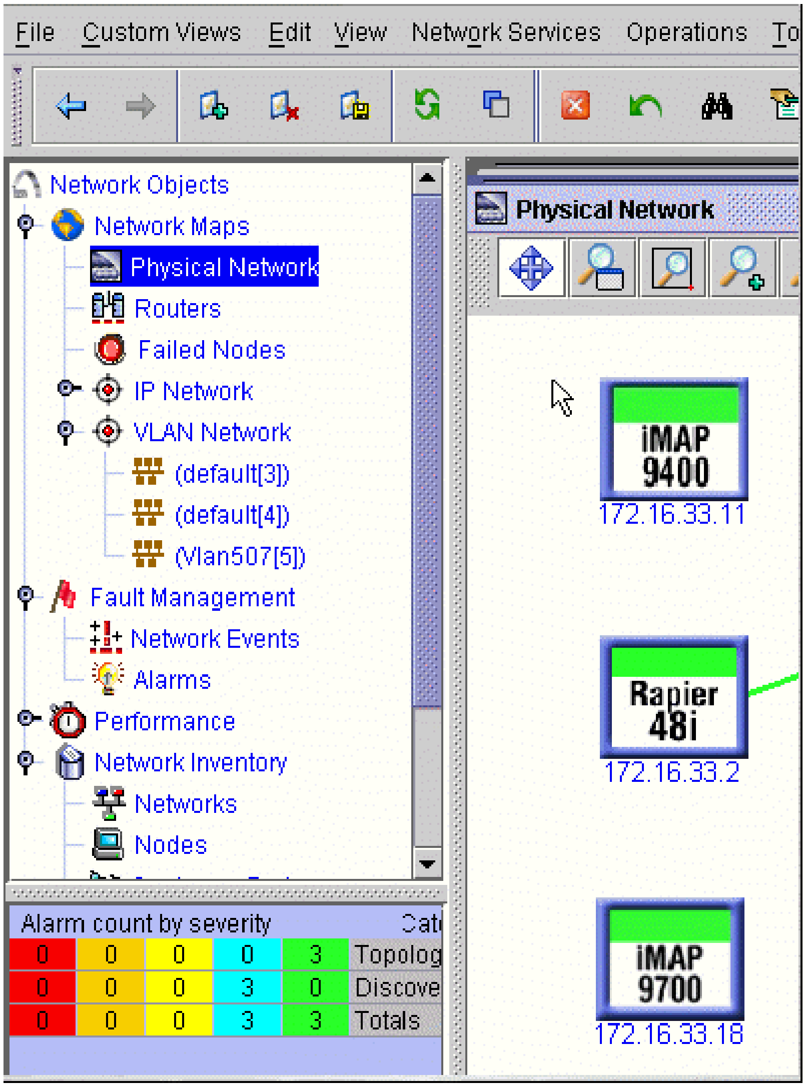


FIGURE 16-29 Sample Island-Based VLAN Networks

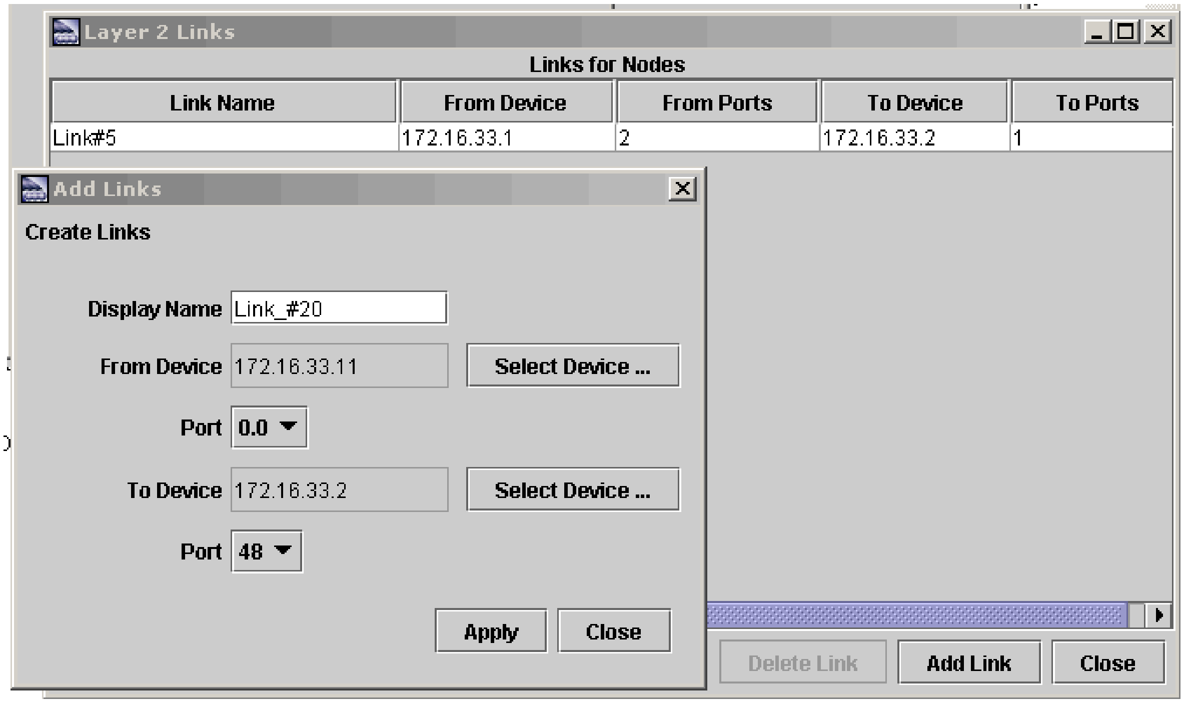
Figure 16-30 shows the three devices on the physical network map. Note that the Rapier 48i already has a physical link to another device.



Alarm count by severity					Cat
0	0	0	0	3	Topolog
0	0	0	3	0	Discove
0	0	0	3	3	Totals

FIGURE 16-30 Three Devices Included in the Island-Based VLAN

To create the physical links, select and Shift-select to include all three devices, and then right-click to select *Network Service -> Link Operation*.The **Layer 2 Links** form appears. Select Add Link, and then select the link name, device number, and port number to configure the example. Figure 16-31 shows Link_#20 being configured.



Links for Nodes

Link Name	From Device	From Ports	To Device	To Ports
Link#5	172.16.33.1	2	172.16.33.2	1

Create Links

Display Name Link_#20

From Device 172.16.33.11

Port 0.0

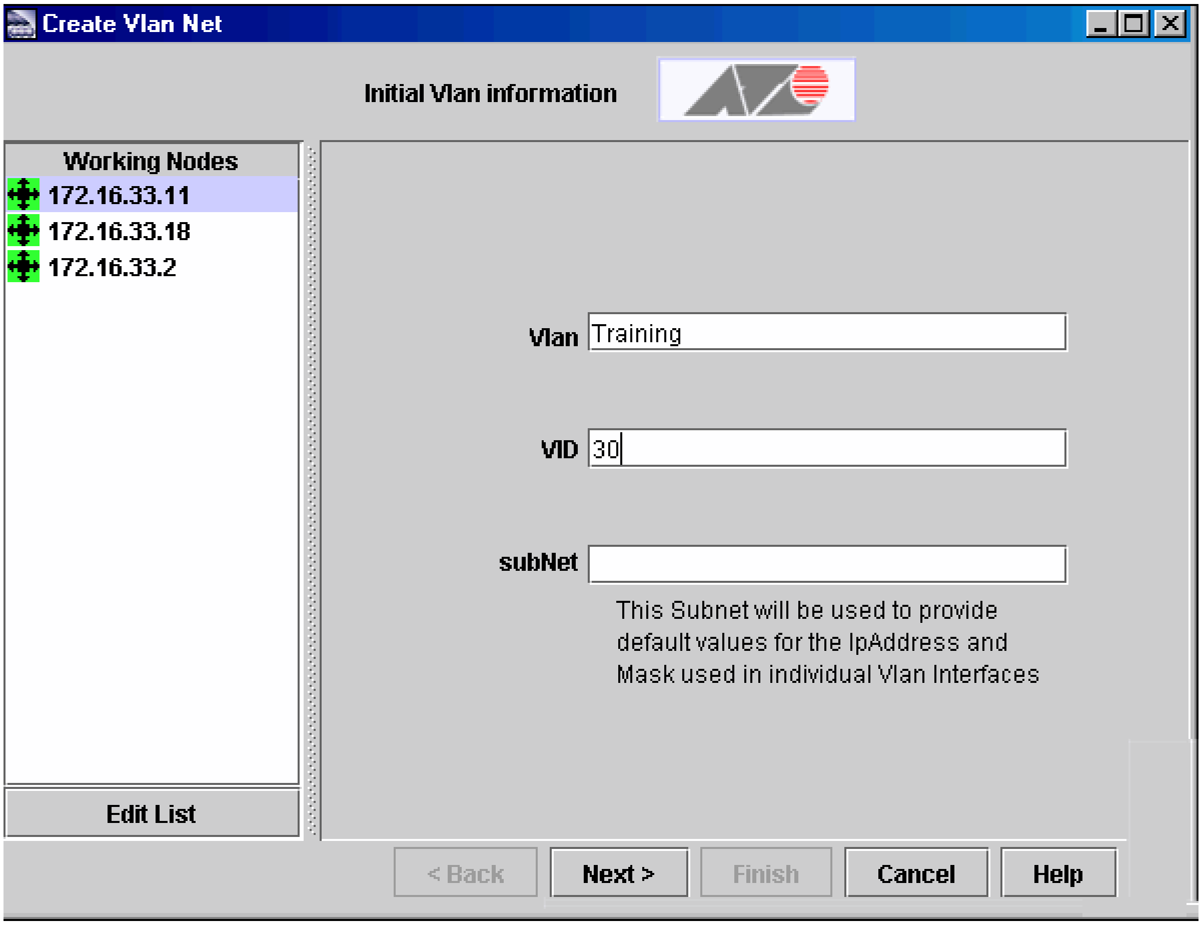
To Device 172.16.33.2

Port 48

FIGURE 16-31 Creating a Physical Link

Once the two physical links (Link_#20 and Link_#21) are created in the AlliedView NMS, the Network VLANs that will use the links (Training and Sales) can be created.

Still on the Physical Network map, Select and shift-select the three devices, and then right-click *Network Services -> VLAN -> Create VLAN*. The Create VLAN form will appear. Fill in the fields for the Training VLAN, as shown in Figure 16-32.



Working Nodes
- 172.16.33.11
- 172.16.33.18
- 172.16.33.2

Vlan: Training

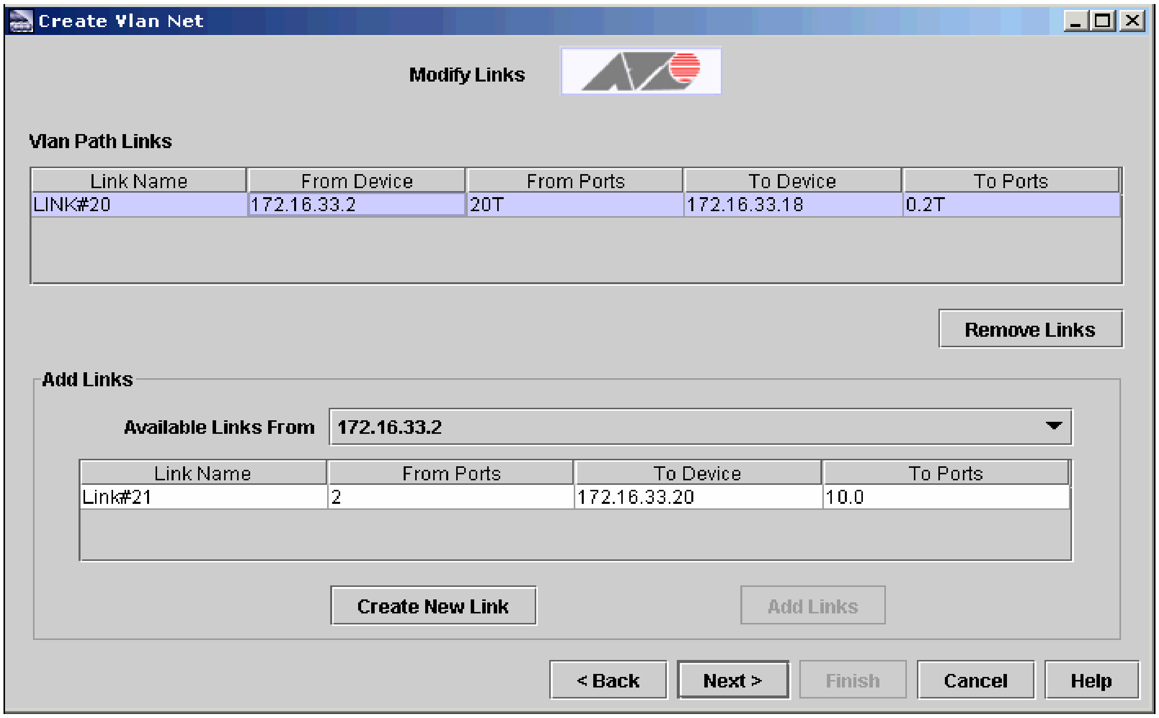
VID: 30

subNet:

This Subnet will be used to provide default values for the IpAddress and Mask used in individual Vlan Interfaces

FIGURE 16-32 Sample Values for the Training Network VLAN

Click **Next**, and the **Modify Links** form appears. Check the checkbox for Link_#20 and Link_#21 from 172.16.33.2. Do not select Link#5, since that is not part of this Network VLAN. Figure 16-33 shows Link_#21 about to be added.



Vlan Path Links

Link Name	From Device	From Ports	To Device	To Ports
LINK#20	172.16.33.2	20T	172.16.33.18	0.2T

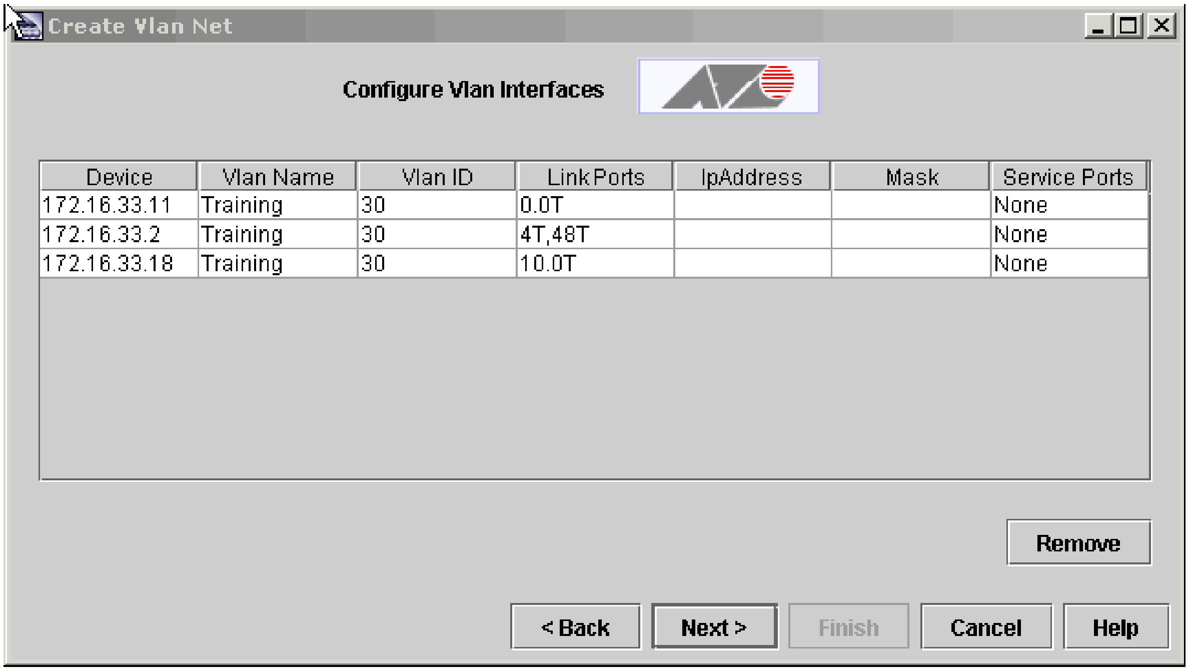
Add Links

Available Links From: 172.16.33.2

Link Name	From Ports	To Device	To Ports
Link#21	2	172.16.33.20	10.0

FIGURE 16-33 Adding Link_#20 and Link_21 to the Network VLAN

After adding the relevant physical links, click **Next**. The **Configure Vlan Interfaces** form appears, and shows the VLAN interfaces over the physical links.



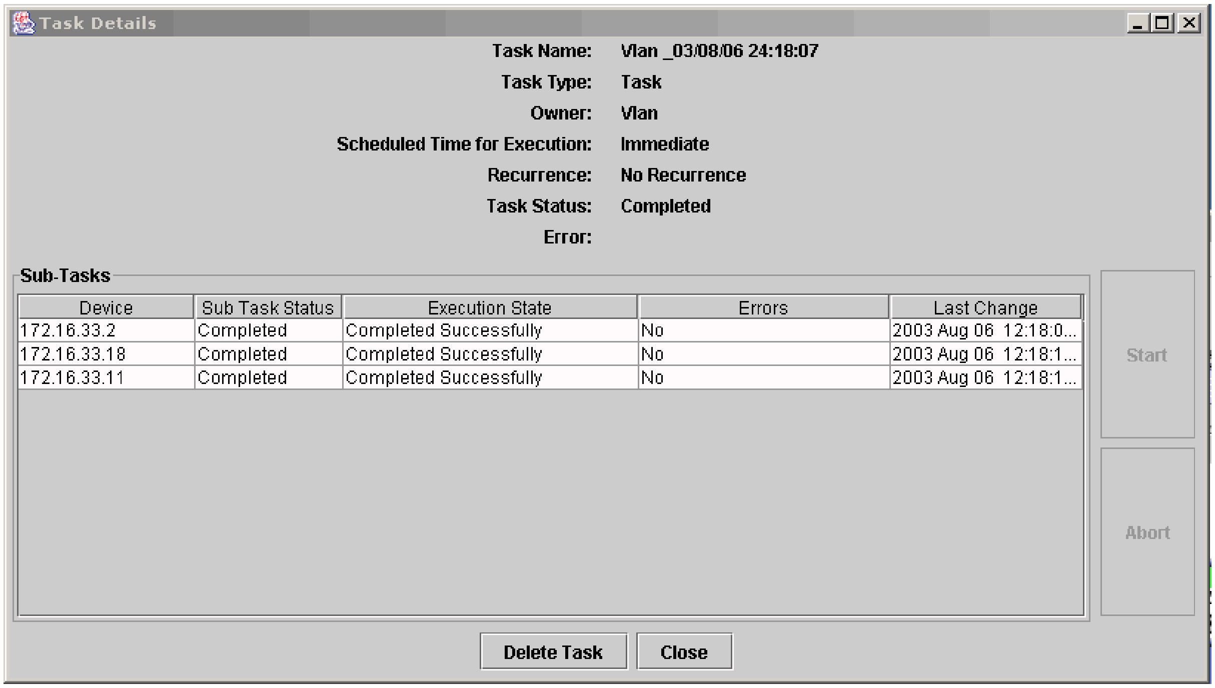
Device	Vlan Name	Vlan ID	Link Ports	IpAddress	Mask	Service Ports
172.16.33.11	Training	30	0.0T			None
172.16.33.2	Training	30	4T,48T			None
172.16.33.18	Training	30	10.0T			None

FIGURE 16-34 Configure Service Ports in Sample Island-Based VLAN

On the **Configure Vlan Interfaces** form, add the service ports (ports that connect to devices that are part of the Training Network VLAN) by clicking in the Service Ports column cell for devices 172.16.33.11 and 172.16.33.18, since these will be the devices that have service ports. In the example the service ports would be 11.0 Untagged for 172.16.33.11 and 0.6 Untagged for 172.16.33.18.

Click **Next**, and the **Test Network VLAN** form appears. This will test the connectivity between all three devices.Click **Finish** and the **Task Details** form will show the tests and if they are successful, as shown in Figure 16-35.

To add the island-based Network VLAN for Sales, the same steps would be followed that would match Figure 16-29.



Task Name: Vlan _03/08/06 24:18:07
Task Type: Task
Owner: Vlan
Scheduled Time for Execution: Immediate
Recurrence: No Recurrence
Task Status: Completed
Error:

Sub-Tasks

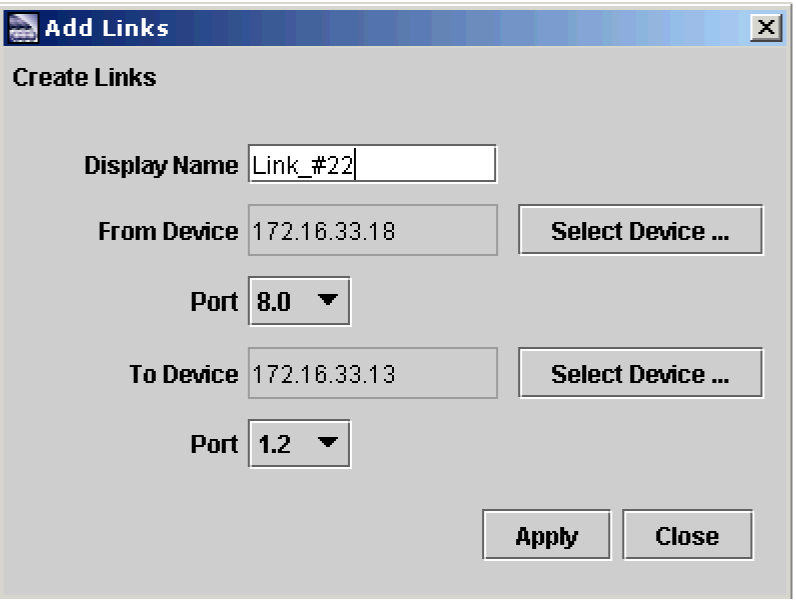
Device	Sub Task Status	Execution State	Errors	Last Change
172.16.33.2	Completed	Completed Successfully	No	2003 Aug 06 12:18:0...
172.16.33.18	Completed	Completed Successfully	No	2003 Aug 06 12:18:1...
172.16.33.11	Completed	Completed Successfully	No	2003 Aug 06 12:18:1...

FIGURE 16-35 Sample Island-Based VLAN Successfully Tested

16.8.2 Extending the Island-Based VLAN

To extend the Network VLAN Training (VID=30), a device (172.16.32.13) will be added to 172.16.32.18, so another physical link will be required between them. A service port will then be added to .18.

First, create a new physical connection. Select (shift-click) both devices, and then select *Network Services -> Link Operations* to invoke the **Layer 2 Links** form. Click **Add Links,** and then choose from among the available links. as shown in Figure 16-36.



Display Name: Link_#22

From Device: 172.16.33.18

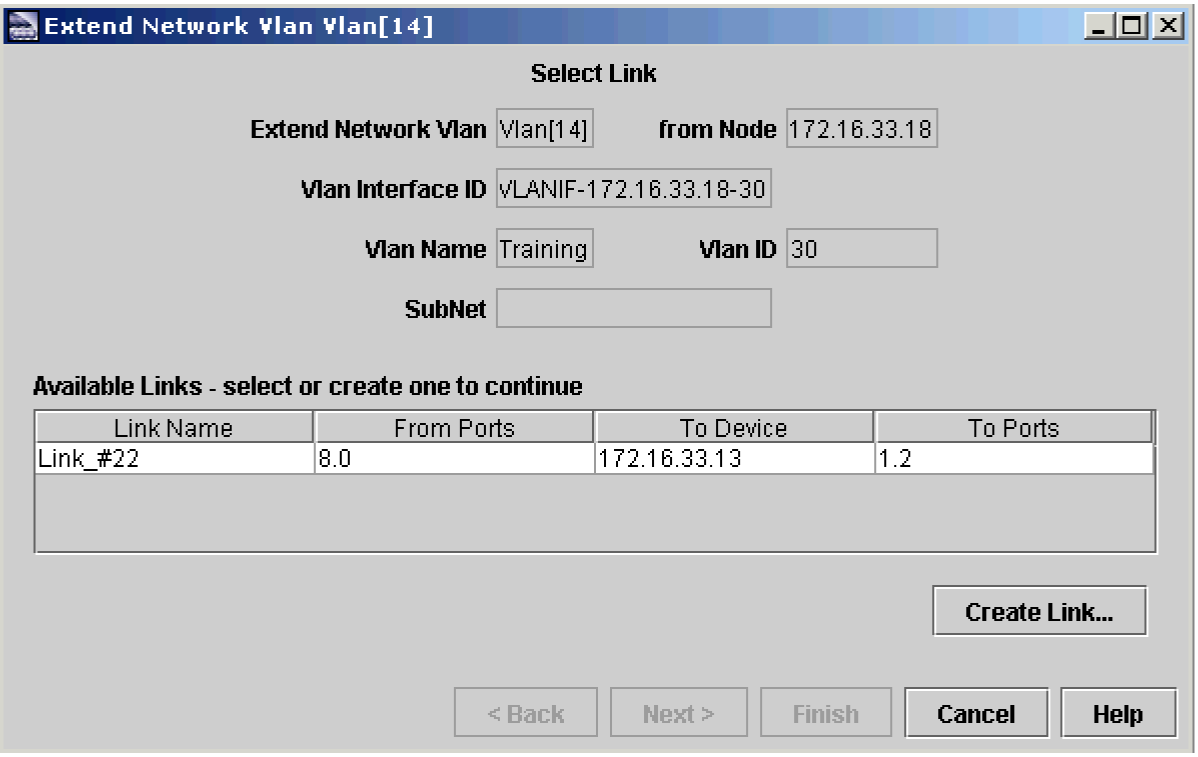
Port: 8.0

To Device: 172.16.33.13

Port: 1.2

FIGURE 16-36 Adding a Physical link to Extend a Network VLAN

Now that the physical link is created, go to the Training VLAN in the VLAN Network map, Right-click on the device in the Network VLAN that has the new link (172.16.33.18) and select *Extend VLAN*. The **Extend Network VLAN** form appears, which includes the new physical link, as shown in Figure 16-37. Note that you could create the new physical link here is desired.



Extend Network Vlan: Vlan[14]

from Node: 172.16.33.18

Vlan Interface ID: VLANIF-172.16.33.18-30

Vlan Name: Training

Vlan ID: 30

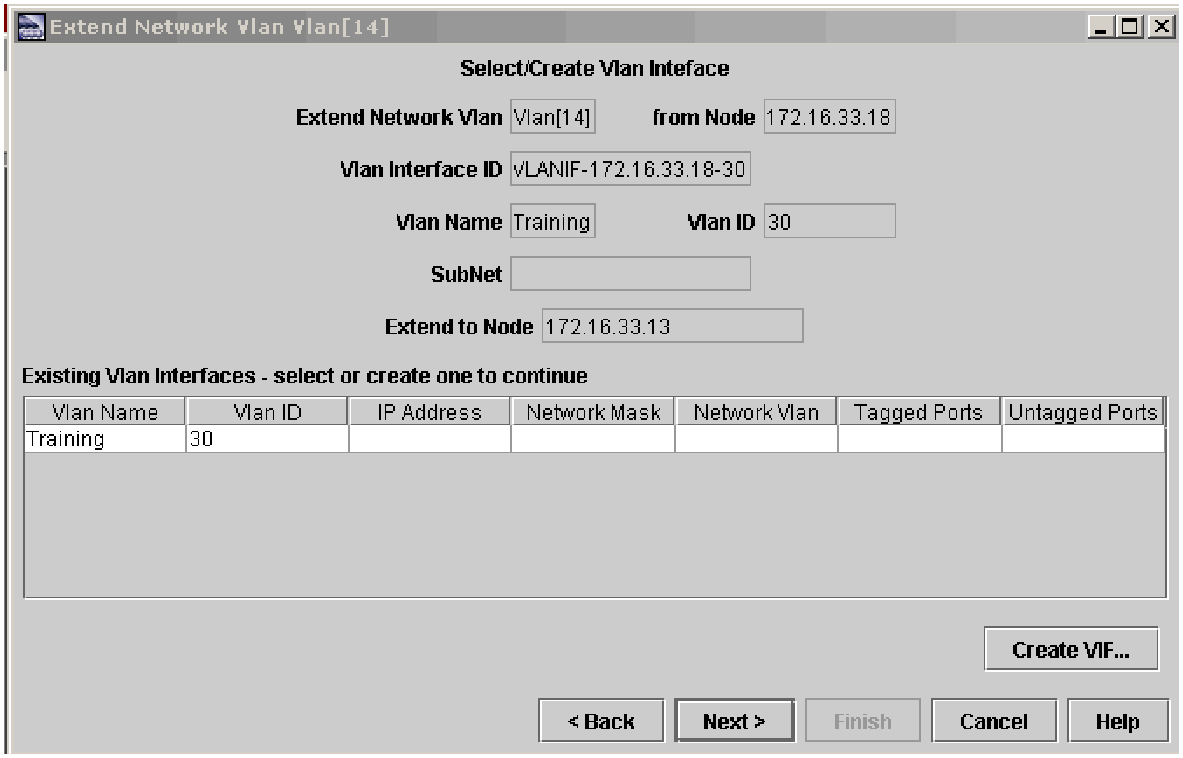
SubNet:

Available Links - select or create one to continue

Link Name	From Ports	To Device	To Ports
Link_#22	8.0	172.16.33.13	1.2

FIGURE 16-37 Selecting a Link for Extending a VLAN

Select the link and click **Next**.The **Select/Create VLAN Interface** form appears. Since the Training VLAN is not yet created on the .13 device, click **Create VIF**. The **Create New VLAN** form appears, with the Training VLAN with the VLAN ID of 30 already filled in. Click **OK** and the VLAN Interface will be added, as shown in Figure 16-38.



Select/Create Vlan Inteface

Extend Network Vlan: Vlan[14] from Node: 172.16.33.18

Vlan Interface ID: VLANIF-172.16.33.18-30

Vlan Name: Training Vlan ID: 30

SubNet:

Extend to Node: 172.16.33.13

Existing Vlan Interfaces - select or create one to continue

Vlan Name	Vlan ID	IP Address	Network Mask	Network Vlan	Tagged Ports	Untagged Ports
Training	30					

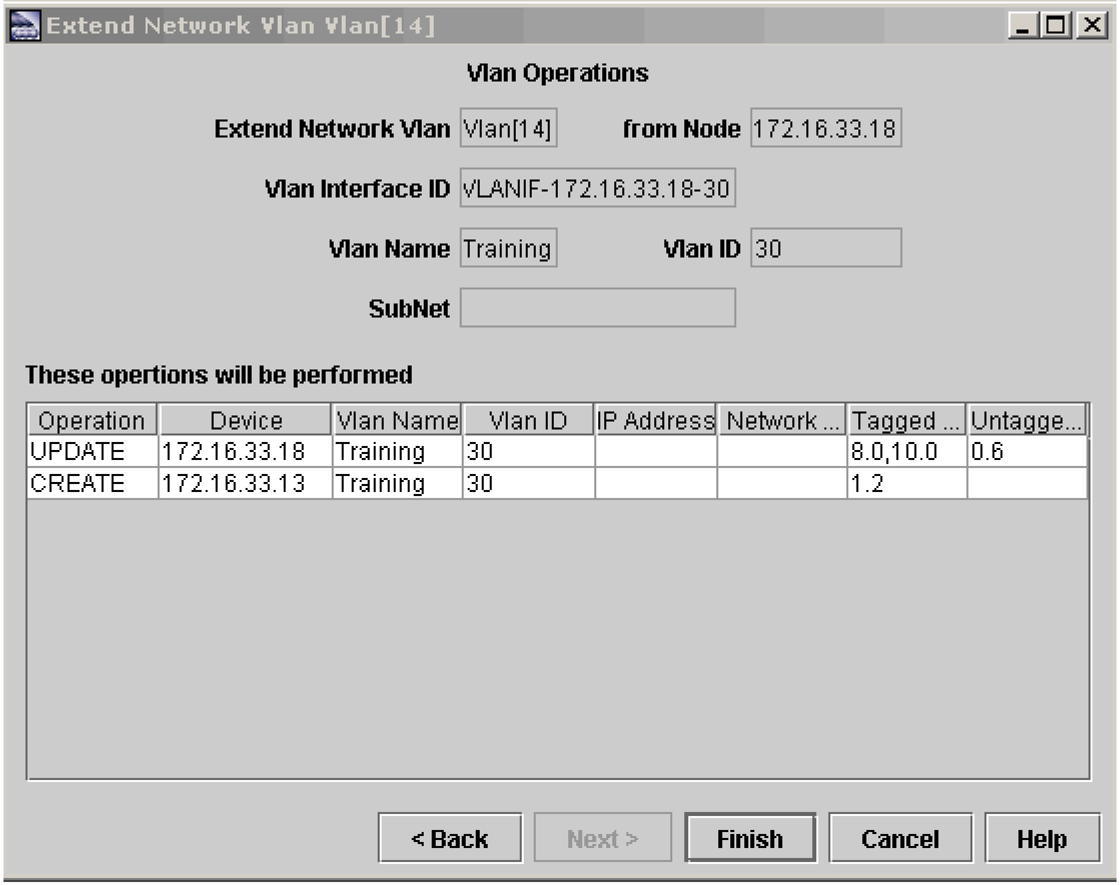
FIGURE 16-38 Creating the VLAN IF on the extended Network VLAN Device

Select the row and click **Next**. The **VLAN Operations** form appears and shows what will be done to finish extending the Network VLAN. Clink **Finish** and the **Task Details** window will perform the operations and give the results.

With the Training Network VLAN now extended, VLAN interfaces on the .13 device can be added that use the Training Network VLAN.

To trim the network VLAN, perform these steps:

1. Go to the specific Network VLAN map. Right-click the device that will no longer have a VLAN IF and select *Configure VLAN Interface*.
2. Select the Training Network VLAN from the pull-down menu, and then put all the tagged and untagged ports back to blank (neither T nor U). Click **Apply**.
3. If any physical links need to be reconfigured since a device is no longer part of this Network VLAN, go to the Physical Network map and delete/add/change links to match the trimmed configuration.



Vlan Operations

Extend Network Vlan: Vlan[14] from Node: 172.16.33.18

Vlan Interface ID: VLANIF-172.16.33.18-30

Vlan Name: Training Vlan ID: 30

SubNet:

These opertions will be performed

Operation	Device	Vlan Name	Vlan ID	IP Address	Network ...	Tagged ...	Untagge...
UPDATE	172.16.33.18	Training	30			8.0,10.0	0.6
CREATE	172.16.33.13	Training	30			1.2	

FIGURE 16-39 Updating the VLAN IF on the Extended Network VLAN Device

16.9 Example Configurations for HVLAN, Translations

16.9.1 Overview

Note: *The Port-based HVLAN and translation feature are not compatible on the same port. Once a port is configured with the HVLAN option, it cannot use the translation feature, and vice-versa. This applies to the cards that support both of these features (GE3, XE1, GE8).*

16.9.2 HVLAN Configuration

Figure 16-40 includes an iMAP 9400, an iMAP 9700, and a Rapier G6. The values seen in this figure will be reflected in the sample steps.

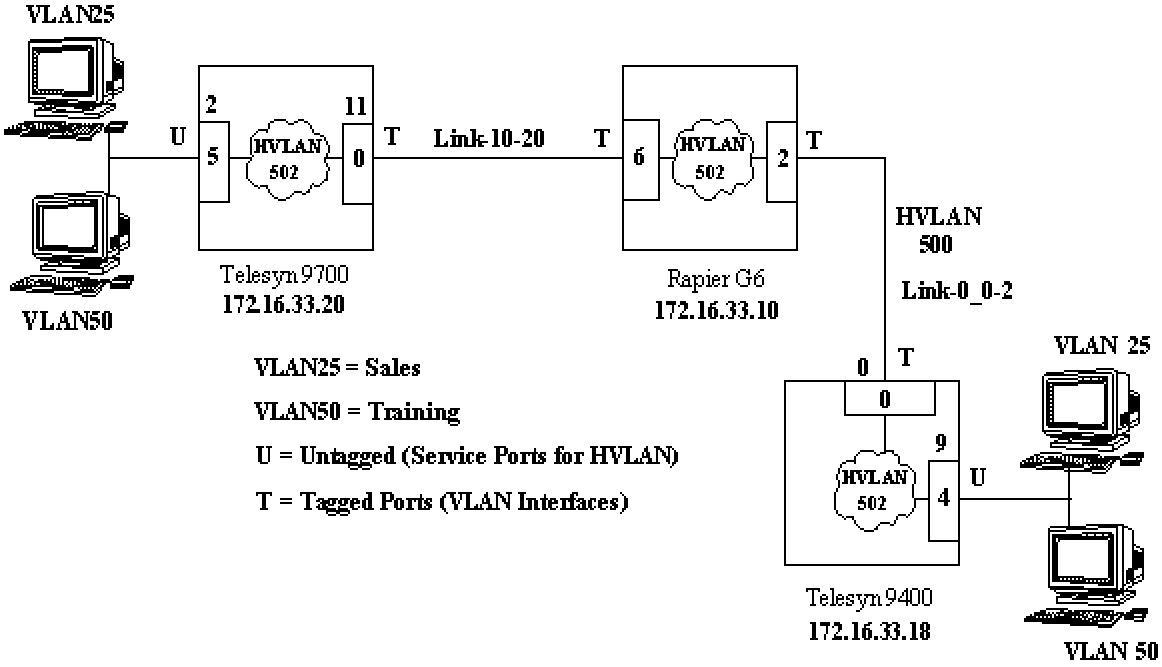
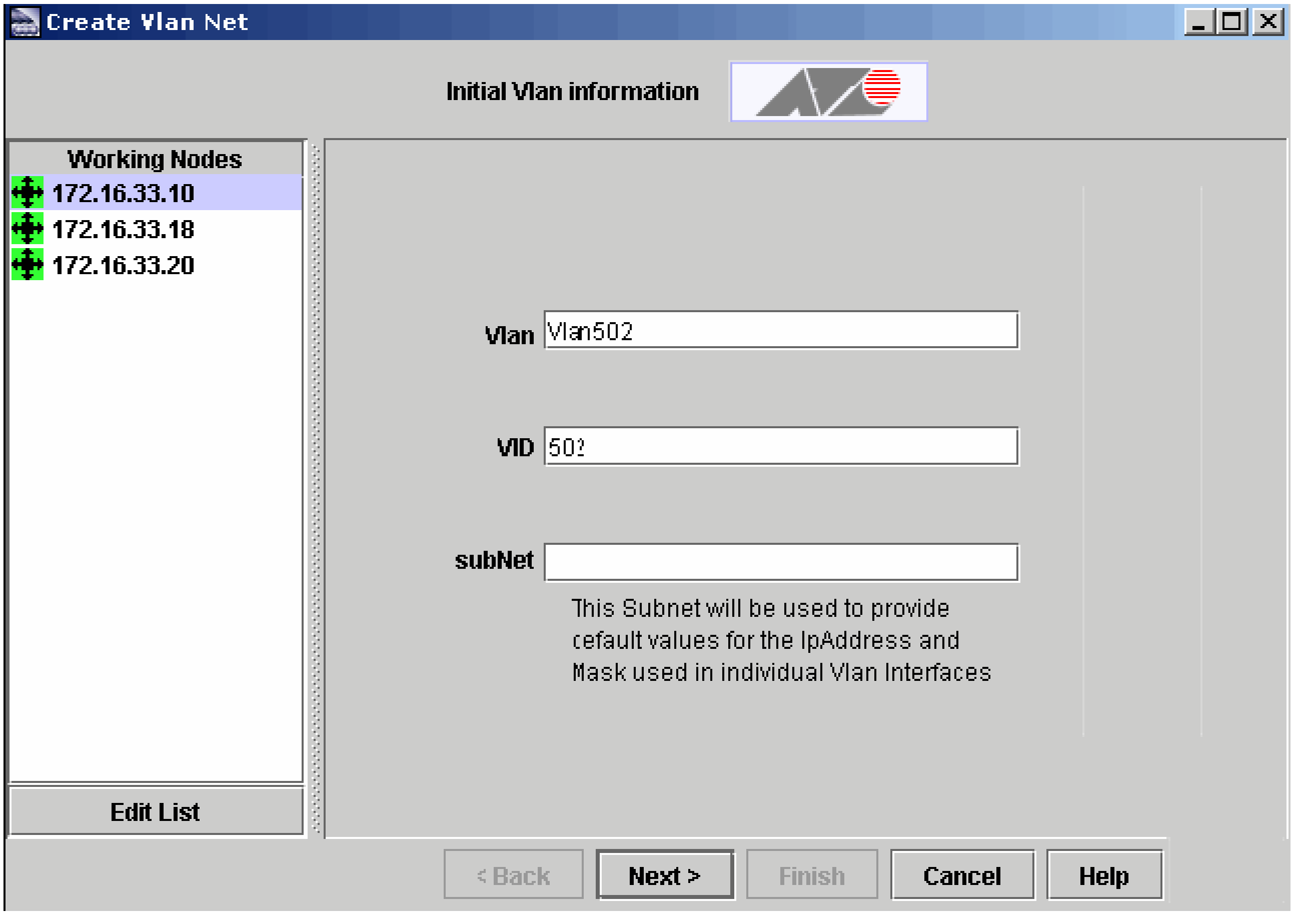


FIGURE 16-40 Example HVLAN Configuration

This example assumes the physical links (Link-10-20 and Link-0_0-2) have already been created, as explained in "Physical Network Map" on page 527. On the Physical Network map, Select and shift-select the three devices, and then right-click *Network Services -> VLAN -> Create VLAN*. The Create VLAN form will appear (Initial VLAN Information). Fill in the fields for the VID502, as shown in Figure 16-41.



Create Vlan Net

Initial Vlan information

Working Nodes
- 172.16.33.10
- 172.16.33.18
- 172.16.33.20

Vlan: Vlan502

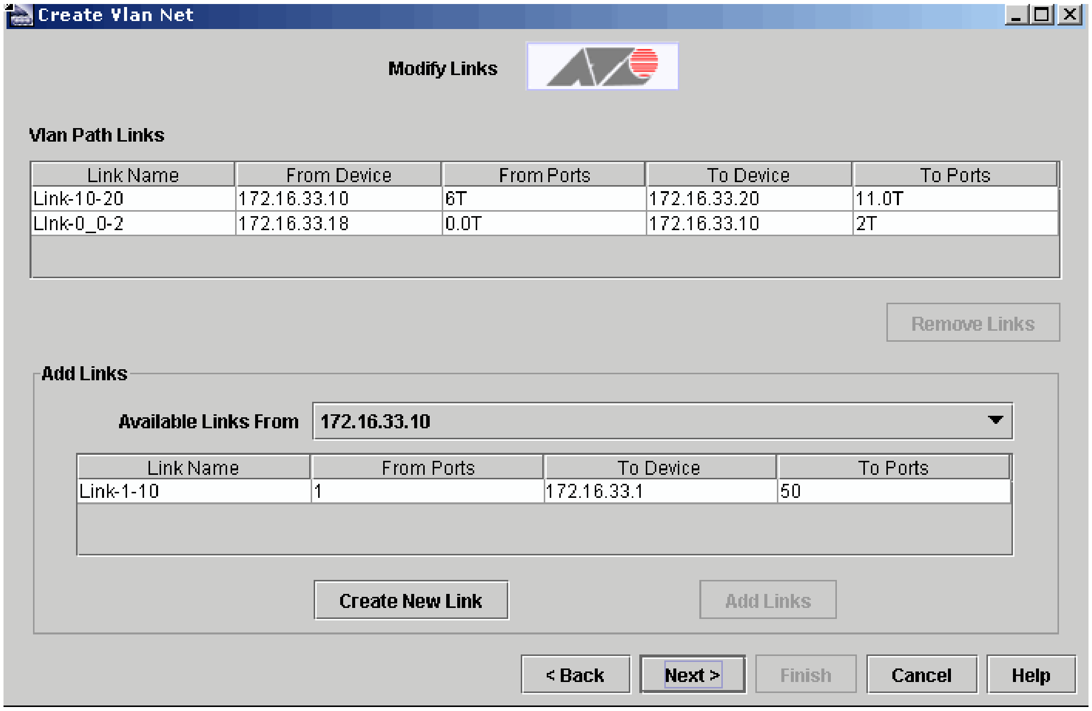
VID: 502

subNet:

This Subnet will be used to provide cefault values for the IpAddress and Mask used in individual Vlan Interfaces

FIGURE 16-41 Create VLAN for HVLAN Configuration

Clicking on Next brings up the Modify Links Form, where the user selects a device from the Available Links Form pull-down, and then adds the appropriate link, as shown in Figure 16-42.



Vlan Path Links

Link Name	From Device	From Ports	To Device	To Ports
Link-10-20	172.16.33.10	6T	172.16.33.20	11.0T
LInk-0_0-2	172.16.33.18	0.0T	172.16.33.10	2T

Available Links From 172.16.33.10

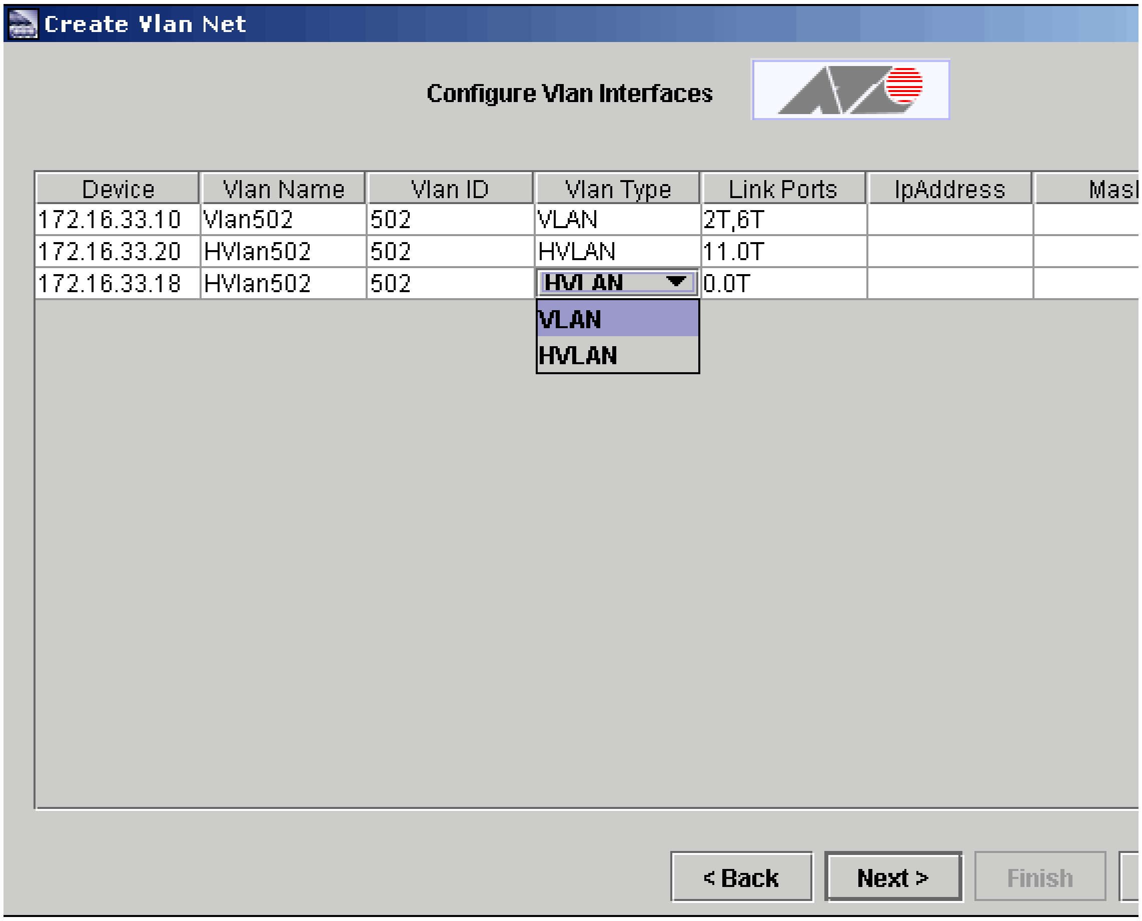
Link Name	From Ports	To Device	To Ports
Link-1-10	1	172.16.33.1	50

FIGURE 16-42 Selecting Links and Adding to the HVLAN Configuration

Clinking **Next** brings up the Configure **VLAN Interfaces Form**, as shown in Figure 16-43. For the iMAP 9000 devices, the type must be changed to HVLAN, which the figure illustrates.

At this point the user can click on the Service Ports column and select which ports will included.

Note: *Service ports that are part of an HVLAN configuration have restrictions, since they must be untagged. Moreover, once a port is a member of any other VLAN (except 1), it cannot be added to the HVLAN configuration.*

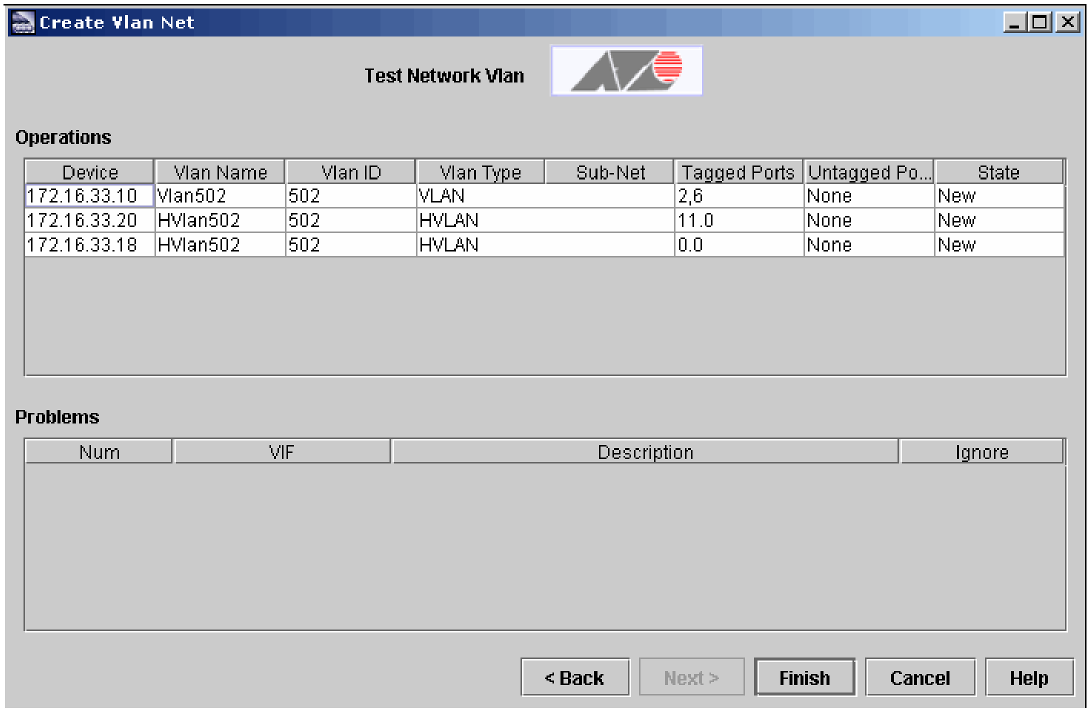


Device	Vlan Name	Vlan ID	Vlan Type	Link Ports	IpAddress	Masl
172.16.33.10	Vlan502	502	VLAN	2T,6T		
172.16.33.20	HVlan502	502	HVLAN	11.0T		
172.16.33.18	HVlan502	502	HVLAN	0.0T		

FIGURE 16-43 Configure Vlan Interfaces Form (iMAP 9000 Devices are Type HVLAN)

Now that the Vlan Interfaces are configured, it can be tested. Clicking on **Next** brings up the Test Network Vlan form, (Figure 16-44), and then clicking on Finish runs the test and provides the results, as shown in Figure 16-45.

If a test does not succeed, an error window appears with a message as to why the test failed.



Test Network Vlan

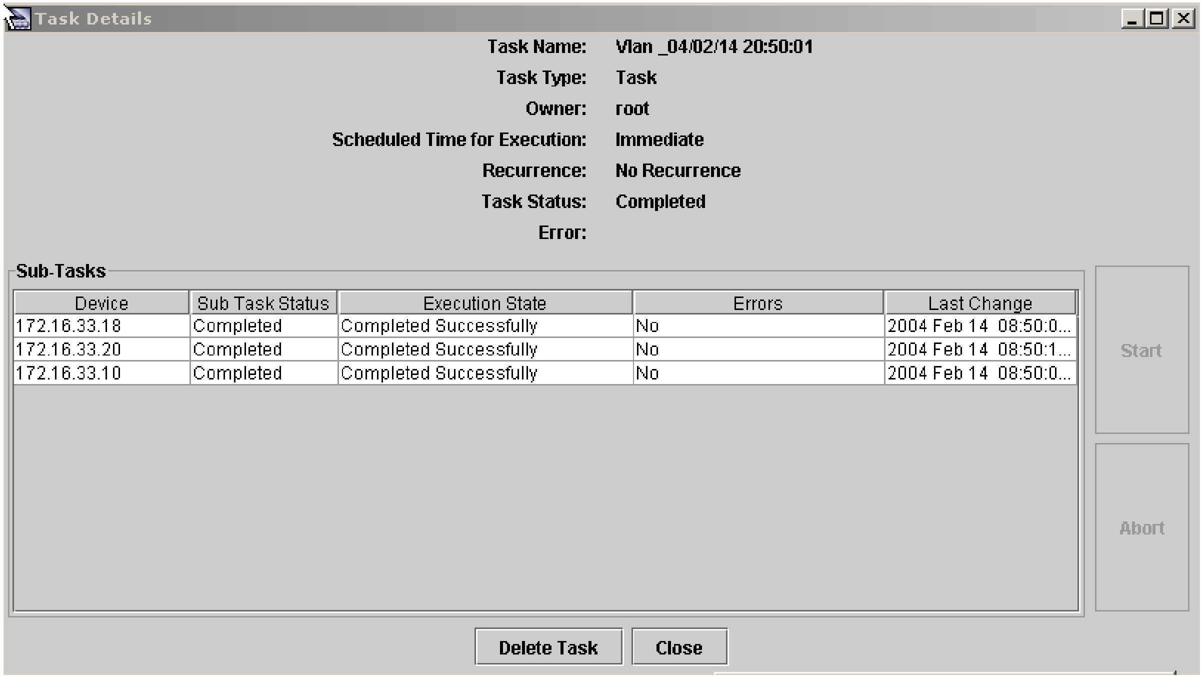
Operations

Device	Vlan Name	Vlan ID	Vlan Type	Sub-Net	Tagged Ports	Untagged Po...	State
172.16.33.10	Vlan502	502	VLAN		2,6	None	New
172.16.33.20	HVlan502	502	HVLAN		11.0	None	New
172.16.33.18	HVlan502	502	HVLAN		0.0	None	New

Problems

Num	VIF	Description	Ignore

FIGURE 16-44 Test Network VLAN Form (Finish to run Test)



Task Name: Vlan _04/02/14 20:50:01
Task Type: Task
Owner: root
Scheduled Time for Execution: Immediate
Recurrence: No Recurrence
Task Status: Completed
Error:

Sub-Tasks

Device	Sub Task Status	Execution State	Errors	Last Change
172.16.33.18	Completed	Completed Successfully	No	2004 Feb 14 08:50:0...
172.16.33.20	Completed	Completed Successfully	No	2004 Feb 14 08:50:1...
172.16.33.10	Completed	Completed Successfully	No	2004 Feb 14 08:50:0...

FIGURE 16-45 Testing Results for the HVLAN Configuration

Extending this HVLAN configuration usually involves adding another iMAP 9000 device with service ports that support multiple VLANs on its untagged ports. The steps are similar to the steps in "Extending the Island-Based VLAN" on page 556, where the user usually creates a link to another device from the VLAN Network node (in the example this would be the **VLAN502[51]** node). The user then right-clicks on the device in the VLAN that has the new link and selects *Extend VLAN*. The link would be selected.

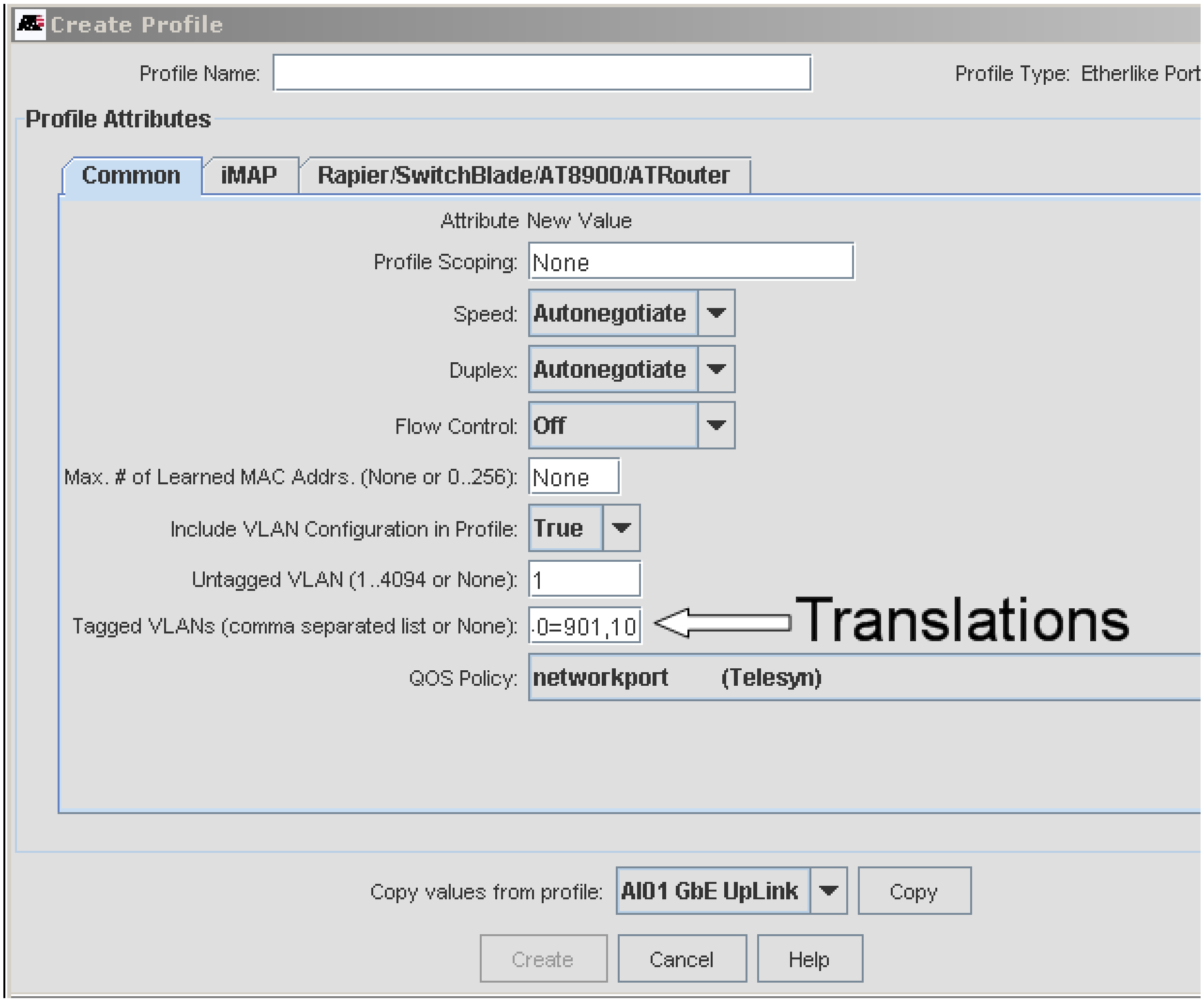
Clicking on **Next** would bring up the **Select/Create Vlan Interface Form**, and the user would select the **Create VIF** button. The VlanID (502) would be given the type HVLAN. After pressing OK, the form would have the new HVLAN502 added to the list. The user would then select this Vlan and select **Next**. The **Vlan Operations Form** appears with the CREATE operation for the HVLAN502. Selecting **Finish** will run the tests to check if the configuration is valid.

16.9.3 VLAN Translations Configuration

16.9.3.1 Setting up VLAN Translations

To set up VLAN translations, the basic sequence is:

1. Create the VLAN that will become the translated VLAN that will go through the network.
2. Associate this translated VLAN with the appropriate interfaces, both on the customer side (where the translation will take place), and the network side (as the translated VLAN goes through the network).
3. Set the translated VLAN option, as shown in the following figure.



Profile Name:
Profile Type: Etherlike Port

Profile Scoping: None
Speed: Autonegotiate
Duplex: Autonegotiate
Flow Control: Off
Max. # of Learned MAC Addrs. (None or 0..256): None
Include VLAN Configuration in Profile: True
Untagged VLAN (1..4094 or None): 1
Tagged VLANs (comma separated list or None): .0=901,10
QOS Policy: networkport (Telesyn)

Copy values from profile: AI01 GbE UpLink

FIGURE 16-46 Port Profile with Translations Options

The values entered are `20=201,40=901,10` (This would be an example for an iMG6x6MOD).

16.9.3.2 Restrictions

Keep the following configuration guidelines in mind when provisioning Translation VLANs:

Note: For more details on the VLAN Translations feature, refer to the Feature Guide.

- The following cards support VLAN translation:

  - GE3, XE1, GE8 (network interfaces) Refer below for FE10/FX10/FX20.
  - ADSL24A/B, SHDSL24, ADSL24SA, ADSL24AE, NTE8, VDSL24A/B, ADSL48A/B (customer interfaces)
- The following cards do **not** support VLAN translation:
  - CES8
- The Port-based HVLAN and translation feature are not compatible on the same port. Once a port is configured with the HVLAN option, it cannot use the translation feature, and vice-versa. This applies to the cards that support both of these features (GE3, XE1, GE8).
- The FE/FX10 does not support both translated and non-translated VLANs on the same port in order to avoid the mixing of a non-translated VLAN traffic onto translated VLAN traffic (which is undesirable) and as such will drop non-translated VLANs. The other card types that support translation do not drop non-translated traffic. Users should be careful in their network design to ensure this.

16.10 Protection Switching-EPSR

16.10.1 Overview of EPSR Topology

In Ethernet-based layer 2 Metropolitan Area Networks (MAN), Spanning Tree Protocol (STP) is normally used to provide redundancy to achieve high availability and continuous access to resources. The iMAP and Allied Telesis Guides explain in detail how STP works and how it is configured.

Starting in AlliedView NMS release 4.1, the GUI can be used to configure another protection switching scheme, the **Ethernet Protection Switched Ring (EPSR)**. EPSR provides a 50 milliseconds switching time for an Ethernet-based ring network, similar to that provided by the Synchronous Optical Network (SONET) protocol. This allows traffic to be redirected around a faulty link in a ring network fast enough to result in an uninterrupted multicast service (such as video).

As the name implies, EPSR protects only those parts of the network that have a ring topology. Each node on the ring will have two Ethernet ports connected to the ring. EPSR operates over these Ethernet ports. Key components that are configured are Control VLANs, Domains, and Protected VLANs.

A *Control VLAN* is configured on the set of devices, and is used to send and receive control messages over the ring network. The devices that are included in the control VLAN make up the **Domain** of the control VLAN.

The VLANs that require fault protection are configured on all the ring ports and are assigned to the EPSR domain. These VLANs are called **Protected VLANs**.

Note: There is only one Control VLAN per EPSR domain and it must use tagged frames. This Control VLAN is unique to this domain and cannot be re-used for another domain.

Note: Control messages use the iMAP Automatic Protection Switching (TAPS) protocol. TAPS protocol control messages are transported around the ring network for an EPSR domain via its control vlan. This is handled internally by the AlliedView NMS.

The protection scheme basically operates by having an EPSR domain on the ring. The vlans that require fault protection are configured on all the ring ports and are assigned to the EPSR domain. The control ring determines if there is a loop, in which case it blocks traffic on the protected VLANs to prevent the loop. If there is no loop, it allows data traffic to flow in either direction.

16.10.1.1 Master and Transit Nodes

One of the nodes in the ring is designated as the **Master node** while all the other nodes are designated as **Transit nodes**. One ring port on the master node is designated to be the *Primary Port* (PP) and the other ring port is designated to be the *Secondary Port* (SP).

When the ring is operating normally, the master node **blocks** its SP port for all non-control traffic (data carried over the protected vlan[s]) belonging to the EPSR domain, preventing a loop on the ring. The layer 2 Ethernet switching and learning mechanisms operate normally on each of the nodes in the ring. However, the control vlan traffic is not blocked at the SP port and is allowed to flow through, because the control messages originate either at a master node or transit node but always terminate at the master node.

When the master node detects a physical link break in the ring, it unblocks its SP port and allows the flow of non-control traffic through the EPSR domain. Once the master node determines that the break in the ring has been restored, it goes back to its normal operating procedure.

16.10.1.2 Example Ring Topologies

A typical topology has all devices (or certain ports on those devices) included in the protection domain. Moreover, each device belongs to only the one domain. However, more complex topologies are possible, as shown in the following figure.

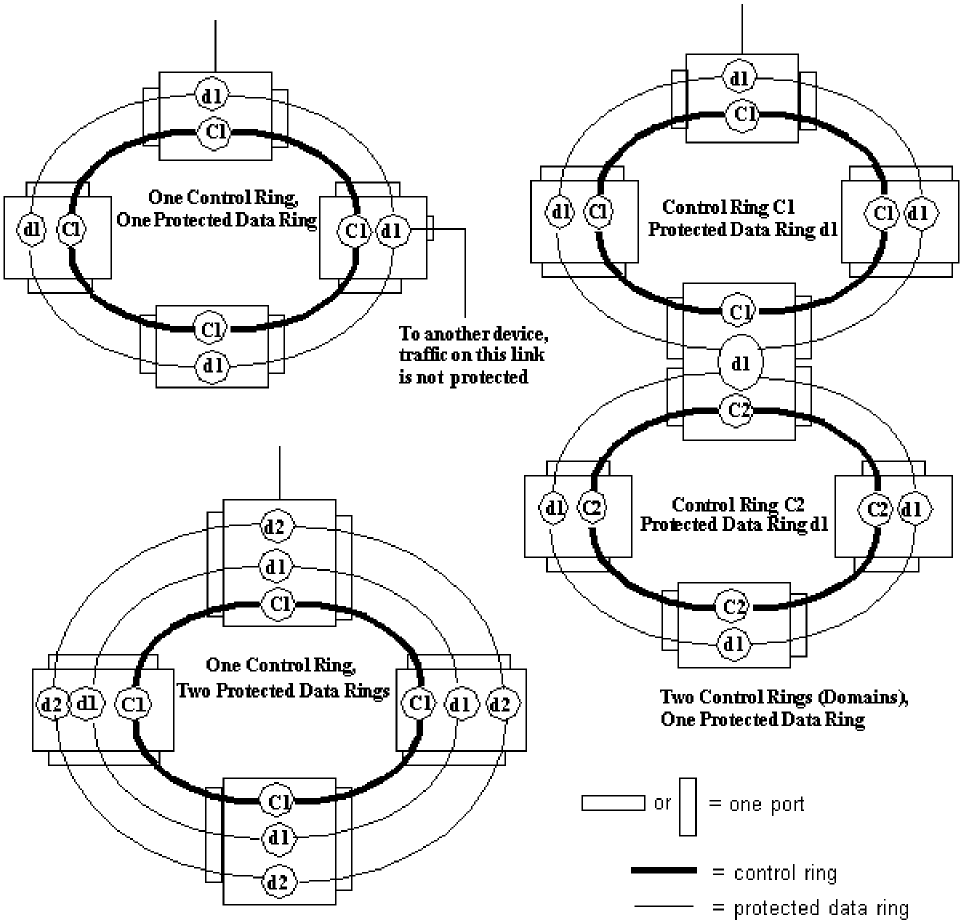


FIGURE 16-47 Example Ring Topologies

16.10.1.3 Summary of EPSR Configuration Data

When the network administrator uses the AlliedView NMS GUI to configure an EPSR topology, the following components are involved. These will be explained in more detail as the AlliedView NMS GUI forms are described and an example configuration is created.

- **Ring Network VLAN** - A VLAN in which the VLAN Interface in each device has two tagged linked ports, and forms a loop.
- **Non-ring Network VLAN** - A VLAN in which the VLAN Interface in each device has two tagged linked ports, and does **not** form a loop. This is a typical network VLAN, but in this case it could be part of a ring that has nodes not managed by the AlliedView NMS.

- **Protected Control Ring** - The network VLAN once it is configured with all the control VLAN attributes.
- **Protected Data Ring** - The network VLAN once it is configured with all the protected VLAN attributes.
- **Control VLAN Interface** - The unique vlan VID which will be used as the control vlan for the EPSR domain.This VLAN is a Network VLAN and can be created as described in "Creating Initial VLAN Information" on page 533.

Note: *Although the network VLAN configured as a loop can be created before configuring an EPSR topology, it is recommended to use the Network VLAN Manager application, since it makes control Vlans easier to create with fewer possible errors, especially since the control VLAN must be configured to form a loop.*

- **Protected VLAN Interface** – The vlan VIDs which require protection on the EPSR domain.
- **VLAN Protection Scheme** - Type of protection you wish for your data network VLANs

Note: *Currently, EPSR is the only protection scheme used.*

- Control Data (part of the TAPS protocol)
  - **HelloTime** – The rate at which the protocol Health control message is sent by the master node for this EPSR domain.
  - **FailOverTime** – Time for which the master node waits before declaring that it has detected a break in the ring for this EPSR domain.
  - **RingFlap Time** – The minimum number of seconds that a master node must remain in the failed state (before moving to the complete state), even if the ring has recovered from its fault condition. This delay is to limit unnecessary blocking and unblocking of the secondary port when a link in the ring is flapping (intermittently recovering from its fault). The default is 0.
- **Link Ports** – The two ports that are members of the EPSR domain.

16.10.2 The Network VLAN Manager Application - Configure Control Ring

Following are the major steps to create an EPSR configuration using the Network VLAN application. The focus will be on the screens and the fields/buttons. A more step-by-step procedure is given in "Example Scenario" on page 579.

16.10.2.1 Create Network VLAN

Part of configuring EPSR is creating Network VLANs that can be configured as control rings or protection rings. The procedure is the same as creating any Network VLAN, as described in "Creating Initial VLAN Information" on page 533.

16.10.2.2 Configure EPS Control Ring

There are two ways to create the control ring using the Network VLAN Manager, depending on what has already been configured:

- **Option 1** - If a Ring Network VLAN has been defined, it can be configured with an EPS protection domain.
- **Option 2** - If a non-Ring Network VLAN has already been defined, it can be extended to form an EPS control ring.

For option 1, if a Ring Network VLAN has been created, it can be configured as an EPS Control Ring by selecting the Network VLAN and choosing the **Configure EPS Control Ring..** option, as shown in the following figure.

Note: *This drop-down is also available from the VLAN maps.*

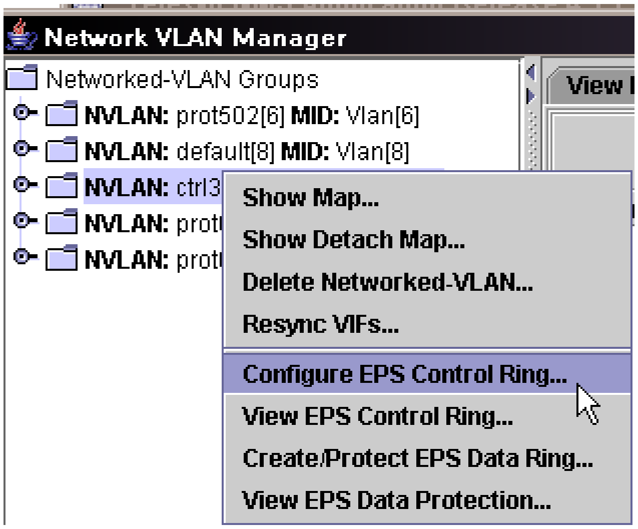
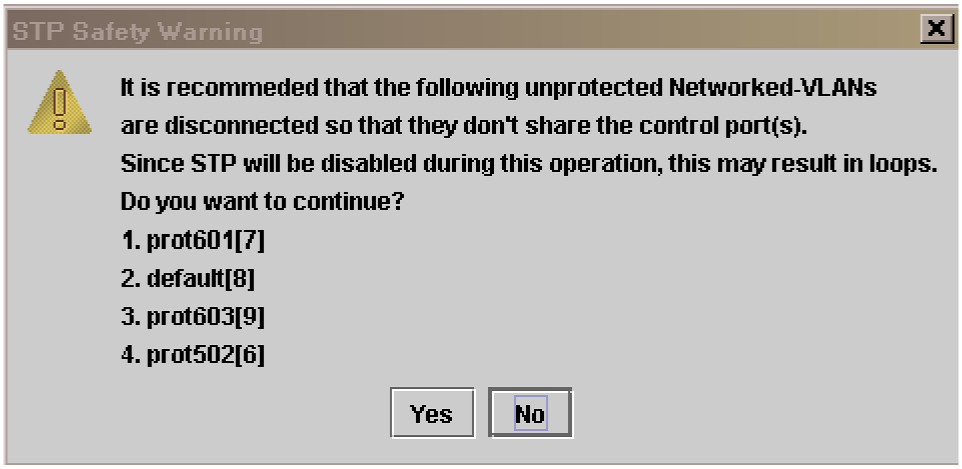


FIGURE 16-48 Pull-Down to Configure EPS Control Ring

Selecting this option brings up the Configure EPS Control Ring Panel. Click on **Create Protection Domain** to bring up the **Create New VLAN Protection Domain** dialog, as shown in Figure 16-50.

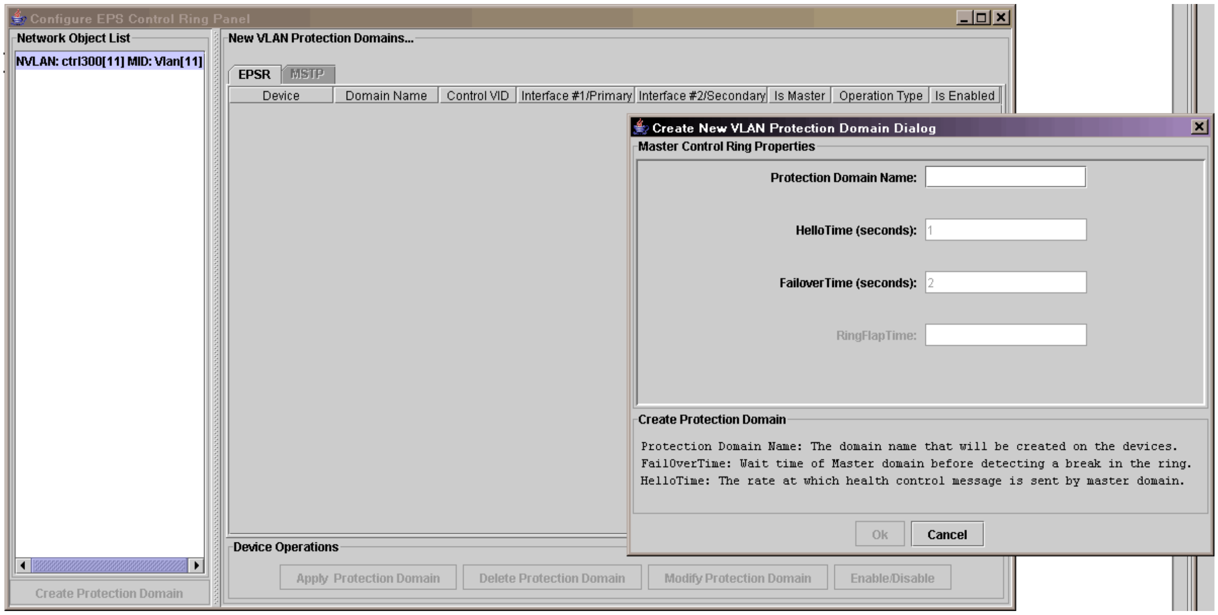
Note: *For AlliedWare Plus devices, which include the SB x908, x900-12X and -24X series, the Protection Domain Name can contain special characters except for percent sign '%'. Although Domain Name with '%' set on the device can be displayed on NMS (Network Inventory - EPSR Domain), its Status will remain Disabled and cannot be Enabled.*

Note: *If there are existing network VLANs on the ports that are going to be used for control ports, clicking on* **Create Protection Domain** *gives the following warning:*


STP Safety Warning

It is recommeded that the following unprotected Networked-VLANs are disconnected so that they don't share the control port(s).
Since STP will be disabled during this operation, this may result in loops.
Do you want to continue?
1. prot601[7]
2. default[8]
3. prot603[9]
4. prot502[6]

FIGURE 16-49 Warning for Creating a Control VLAN



Protection Domain Name:

HelloTime (seconds): 1

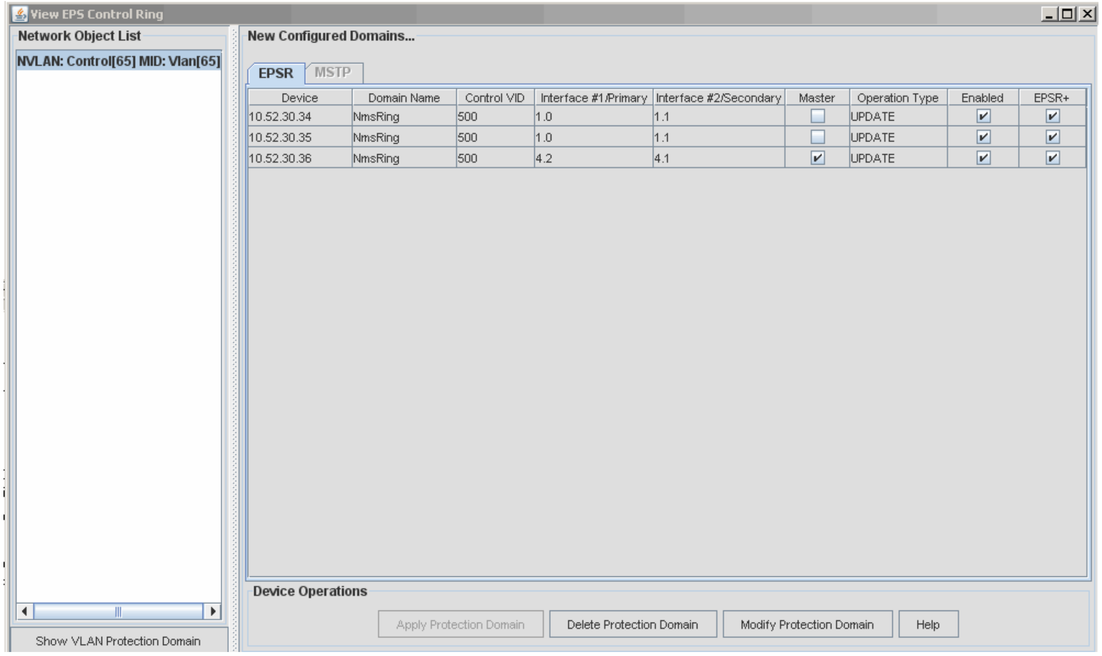
FailoverTime (seconds): 2

RingFlapTime:

```
Protection Domain Name: The domain name that will be created on the devices.
FailOverTime: Wait time of Master domain before detecting a break in the ring.
HelloTime: The rate at which health control message is sent by master domain.
```

FIGURE 16-50 Configure EPS Control Ring Panel

After filling in the fields, click on **OK** to bring up the list of all EPS domains that will be configured on each device. The columns in the EPSR Protection Domain panel are filled in, as shown in the following figure.



Device	Domain Name	Control VID	Interface #1/Primary	Interface #2/Secondary	Master	Operation Type	Enabled	EPSR+
10.52.30.34	NmsRing	500	1.0	1.1	□	UPDATE	☑	☑
10.52.30.35	NmsRing	500	1.0	1.1	□	UPDATE	☑	☑
10.52.30.36	NmsRing	500	4.2	4.1	☑	UPDATE	☑	☑

FIGURE 16-51 Creating Control Ring (Apply Protection Domain)

The user at this point can change the following attributes of the control ring (refer to Table 16-7).

- Interface #1/Primary (whichever one is chosen as the Primary)
- Is Master
- Is Enabled

- EPSR+ - Enhanced Recovery, this is defaulted to the recommended settings, and is disabled if unavailable on the node software release.

Note: Refer to the Allied Telesis Software Manuals for detailed information about the EPSR+ feature.

Finally, the user clicks **Apply Protection Domain**. This configures the devices to support the control ring. The Task Details window appears and the control ring is configured for each device. (If there is an error, the Task Details window can be used to determine the error condition.)

Once the Protection Domain is applied, a map of the control ring is created that can be viewed, as shown in subsection "Show EPS Control Ring Map" on page 575.

Table 16-7 summarizes the fields for the Configure EPS Control Ring Panel

TABLE 16-7 **Fields for the Configuration of the EPS Control Ring Panel**

Option	Purpose
Network Object List	Network VLAN Object that is being used to configure the control ring. The format is: NVLAN:<name of network vlan>[ID]<MID:Vlan[ID] The ID is the way to uniquely identify the network VLAN.
Create Protection Domain	Brings up the Create New Protection VLAN Domain Dialog.
Create New Protection VLAN Domain Dialog	**Protection Domain** - The name of the domain that will include all of the devices that are part of the Network VLAN. Naming conventions are up to 15 characters (spaces not allowed). **Hello Time** and **Failover Time** - Refer to "Summary of EPSR Configuration Data" on page 568. **RingFlap Time**:

TABLE 16-7 Fields for the Configuration of the EPS Control Ring Panel

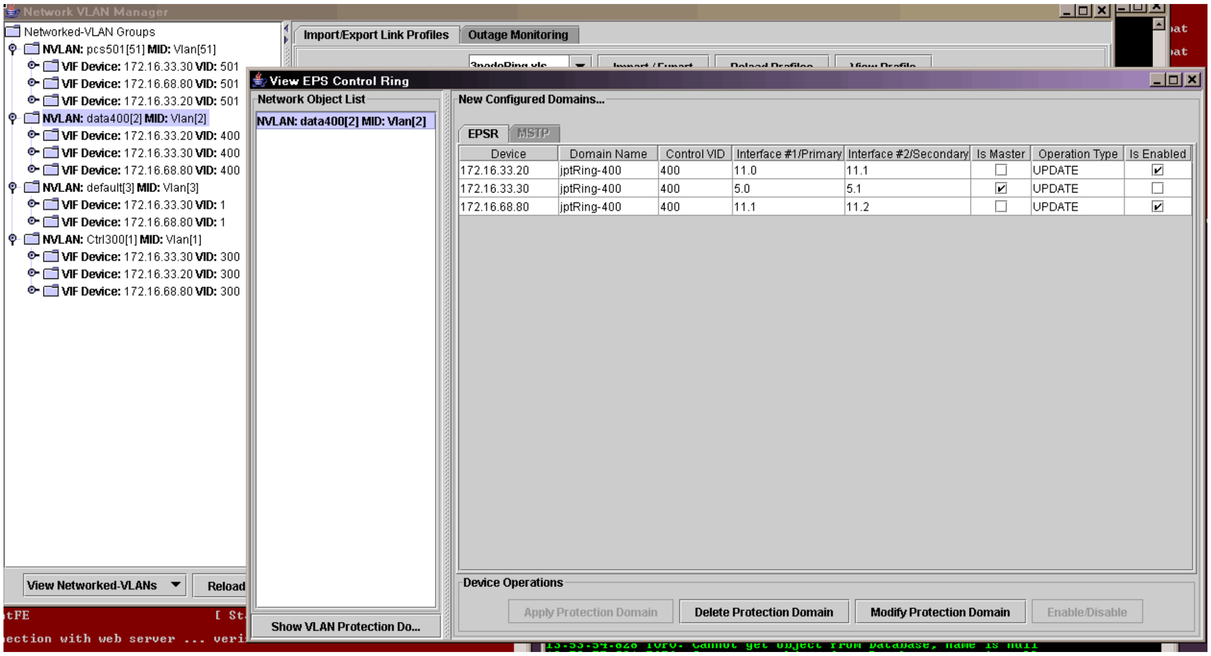
Option	Purpose
EPSR Protection Domain panel	Lists the relevant information for the control ring: Have control over columns that are enabled. (Controllable fields in **bold**.) Device: The name of the device as defined in the Managed Object Properties Domain Name: The domain name that applies to this specific Network VLAN and all of its associated nodes. Control VID: The VID of the network VLAN that is being used to create the protection ring. **Interface #1/Primary** - Can toggle between Primary and Secondary. Interface #2/Secondary **Is Master**: Selects which device is to be the master node. This is usually the node that is connected to upstream devices. (This cannot be modified if you are modifying an existing control ring.) Operation Type: The operation (such as Create) that is being applied to the ring configuration. **Is Enabled**: Checked by default, allows the user to disable the EPS domain for that device. Note the ring (master node) should be disabled only to perform a configuration change. If the master is disabled, the ring will not provide protection. It appears that the device blocks both ports so it no longer is connected to the other devices (and the ring is broken). If the transit is disabled it also appears that the device blocks both ports for protected traffic so it no longer is connected to other devices (although the ring except for that device will still function). **EPSR+** - Enhanced Recovery, this is defaulted to the recommended settings, and is disabled if unavailable on the node software release.
Device Operations	Options to perform on the created control VLAN: **Apply Protection Domain** - Configures the devices to support the control ring. Brings up the Task Details window. **Delete Protection Domain** -Activated only when the EPS Control Ring has already been created, allows the user to delete the protection domain for the network VLAN. Note that the network VLAN itself is not deleted. Refer to "View/Modify/Delete EPS Control RIng" on page 573. **Modify Protection Domain** - Activated only when the EPS Control Ring has already been created, allows the user to modify the protection domain for the network VLAN. Refer to "View/Modify/Delete EPS Control RIng" on page 573. **Enable/Disable** - Activated only when the EPS Control Ring has already been created, allows the user to disable the protection domain after it has been applied, and vice versa. Refer to "Enable/Disable EPS Control Ring" on page 574.

If **Apply Protection Domain** is chosen, the devices that use the Network VLAN are included in the Configure EPS Control Ring window, and in configuring the Control Ring the AlliedView NMS will complete the loop.

16.10.2.3 View/Modify/Delete EPS Control RIng

Once a control ring has been created, it can be viewed by selecting the relevant networked VLAN and selecting View EPS Control Ring. The View EPS Control Ring window appears, with the attributes of the control ring included in the New Configured Domains panel. Refer to the following figure.

Note: In release 12.0, the EPSR+ field is included as well.


Network VLAN Manager
Networked-VLAN Groups
NVLAN: pcs501[51] MID: Vlan[51]
VIF Device: 172.16.33.30 VID: 501
VIF Device: 172.16.68.80 VID: 501
VIF Device: 172.16.33.20 VID: 501
NVLAN: data400[2] MID: Vlan[2]
VIF Device: 172.16.33.20 VID: 400
VIF Device: 172.16.33.30 VID: 400
VIF Device: 172.16.68.80 VID: 400
NVLAN: default[3] MID: Vlan[3]
VIF Device: 172.16.33.30 VID: 1
VIF Device: 172.16.68.80 VID: 1
NVLAN: Ctrl300[1] MID: Vlan[1]
VIF Device: 172.16.33.30 VID: 300
VIF Device: 172.16.33.20 VID: 300
VIF Device: 172.16.68.80 VID: 300
View Networked-VLANs
Reload
Import/Export Link Profiles
Outage Monitoring
View EPS Control Ring
Network Object List
NVLAN: data400[2] MID: Vlan[2]
Show VLAN Protection Do...
New Configured Domains...
EPSR
MSTP
Device Operations
Apply Protection Domain
Delete Protection Domain
Modify Protection Domain
Enable/Disable

Device	Domain Name	Control VID	Interface #1/Primary	Interface #2/Secondary	Is Master	Operation Type	Is Enabled
172.16.33.20	jptRing-400	400	11.0	11.1	☐	UPDATE	☑
172.16.33.30	jptRing-400	400	5.0	5.1	☑	UPDATE	☐
172.16.68.80	jptRing-400	400	11.1	11.2	☐	UPDATE	☑

FIGURE 16-52 View EPSR Control Ring Panel

The Delete and Modify buttons are now activated. To modify the control ring, the user can choose one of the editable fields (explained in Table 16-7) and select **Modify Protection Domain.** The task list window will appear as the application changes the Control Ring attributes for each device.

To delete the control ring, the user selects **Delete Protection Domain.** After a confirmation message appears, the control ring and its attributes are deleted.

Note: The Delete Protection Domain operation deletes only the EPS domain associated with the ring, but not the Loop Networked VLAN.

16.10.2.4 Enable/Disable EPS Control Ring

Refer to Table 16-7.

16.10.2.5 Show EPS Control Ring Map

Once a valid control ring is configured, selecting the Network VLAN and right clicking on **Show (Detached) Map** brings up an icon map that shows the devices and links and their associated states. This figure can also be shown by clicking on the Network VLAN under the VLAN Network node. Refer to the following figure.

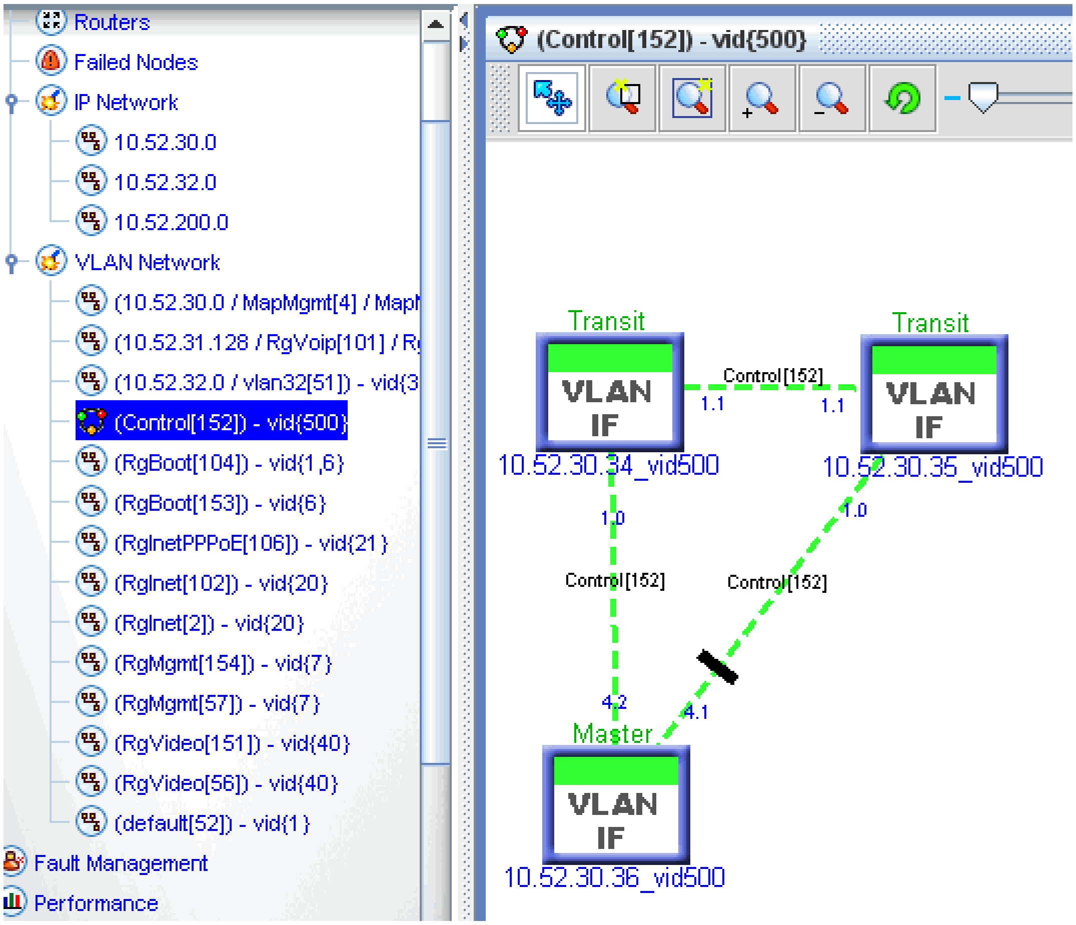


FIGURE 16-53 Control Ring Map

If a VLAN Interface (VLAN IF) has been added to an EPSR Domain on a device, then the Vlan Map symbol for that control VLAN IF will show its Domain role, either **Transit** or **Master**, above the symbol.

The state of the EPSR Domain is reflected in the color of the text of the domain role as follows:

For a Master VLAN IF:

- IDLE is gray (This indicates that the Domain is disabled)
- COMPLETE is green
- FAILED is red

Note: *For AlliedWare Plus devices, which include the SB x908, x900-12X and -24X series, the initial state of the master node is idle (gray), and turns to green only after the associated transit nodes have been discovered. The amount of time this takes depends on the number of transit nodes that make up the ring.*

For Transit VLAN IF;

- IDLE is gray (This indicates that the Domain is disabled)
- LINKS-UP is green

- LINKS-DOWN is red
- PRE-FORWARDING is orange

16.10.3 The Network VLAN Manager Application - Configure Data Ring

16.10.3.1 Create/Protect EPS Data Ring

Usually, once the EPS Control Ring is created and configured (with its domain), a new EPS Data ring is created. There are several ways to create this data protection ring, depending on what has already been configured:

- **Option 1** - If a control ring has already been defined, it can be cloned to create a new protected data network VLAN (protected data ring). The protection ring matches the ports, devices (and therefore the domain) of the control ring.
- **Option 2** - If a non-ring data network VLAN has already been defined, it can be associated with one of its possible control rings; since the data network VLAN is not a ring, the application will complete the data protection ring (and create any additional VLAN Interfaces as well).
- **Option 3** - If a ring data network VLAN has already been defined, it can be associated with one of its possible control rings and labeled as protected.

For option 1, the network VLAN that is a control ring is selected and right-clicked on **Create/Protect EPS Data Ring...** as shown in the following figure.

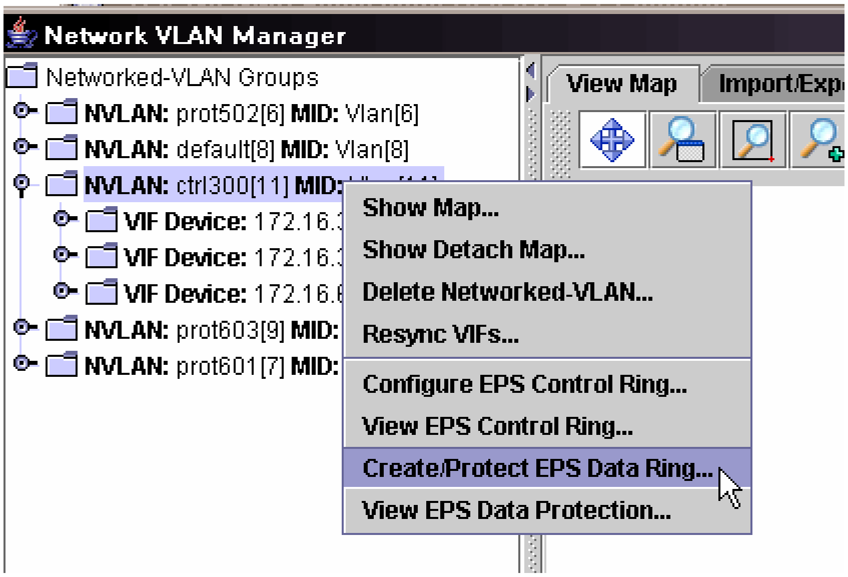
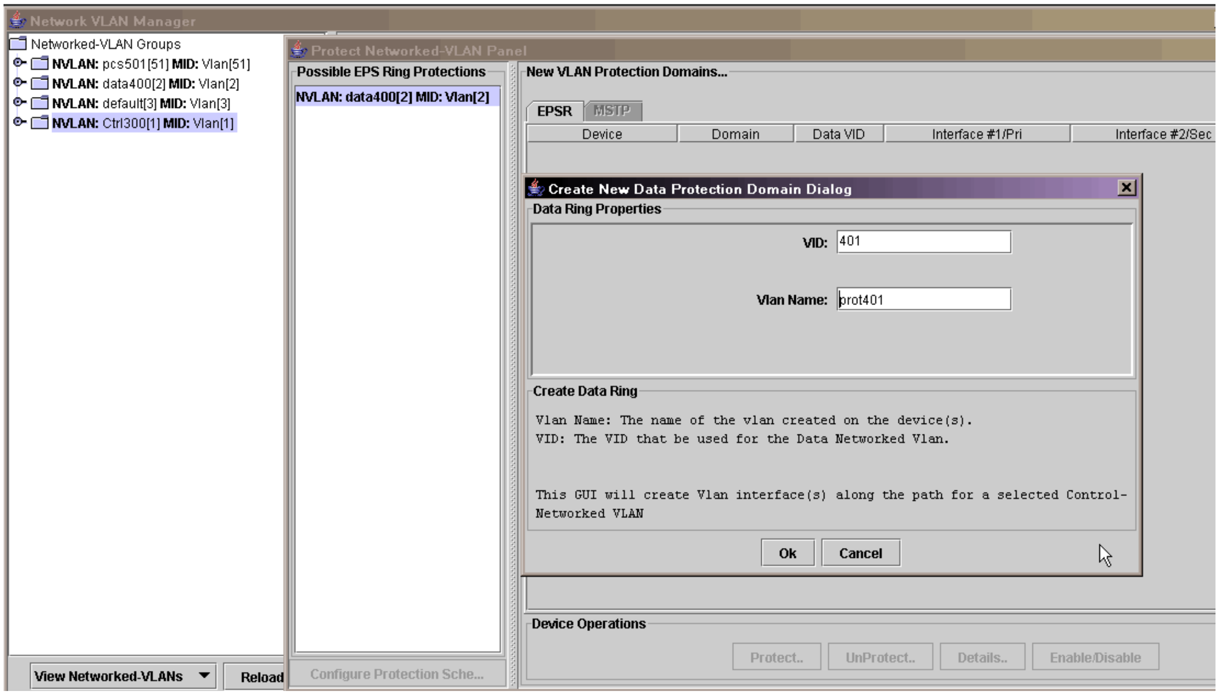


FIGURE 16-54 Creating an EPS Data Protection Ring by Copying a Control Network VLAN

In the Protection Ring Configuration Panel, the user selects **Configure Protection Scheme** The Network VLAN Manager creates a “copy” of the control network VLAN (meaning creates a network VLAN that follows the same path as the selected Control VLAN), and brings up the create data ring dialog to assign a data VID. Refer to the following figure.


Network VLAN Manager
Networked-VLAN Groups
NVLAN: pcs501[51] MID: Vlan[51]
NVLAN: data400[2] MID: Vlan[2]
NVLAN: default[3] MID: Vlan[3]
NVLAN: Ctrl300[1] MID: Vlan[1]
View Networked-VLANs
Reload
Protect Networked-VLAN Panel
Possible EPS Ring Protections
NVLAN: data400[2] MID: Vlan[2]
Configure Protection Sche...
New VLAN Protection Domains...
EPSR
MSTP
Device
Domain
Data VID
Interface #1/Pri
Interface #2/Sec
Create New Data Protection Domain Dialog
Data Ring Properties
Create Data Ring
Ok
Cancel
Device Operations
Protect..
UnProtect..
Details..
Enable/Disable

VID: 401

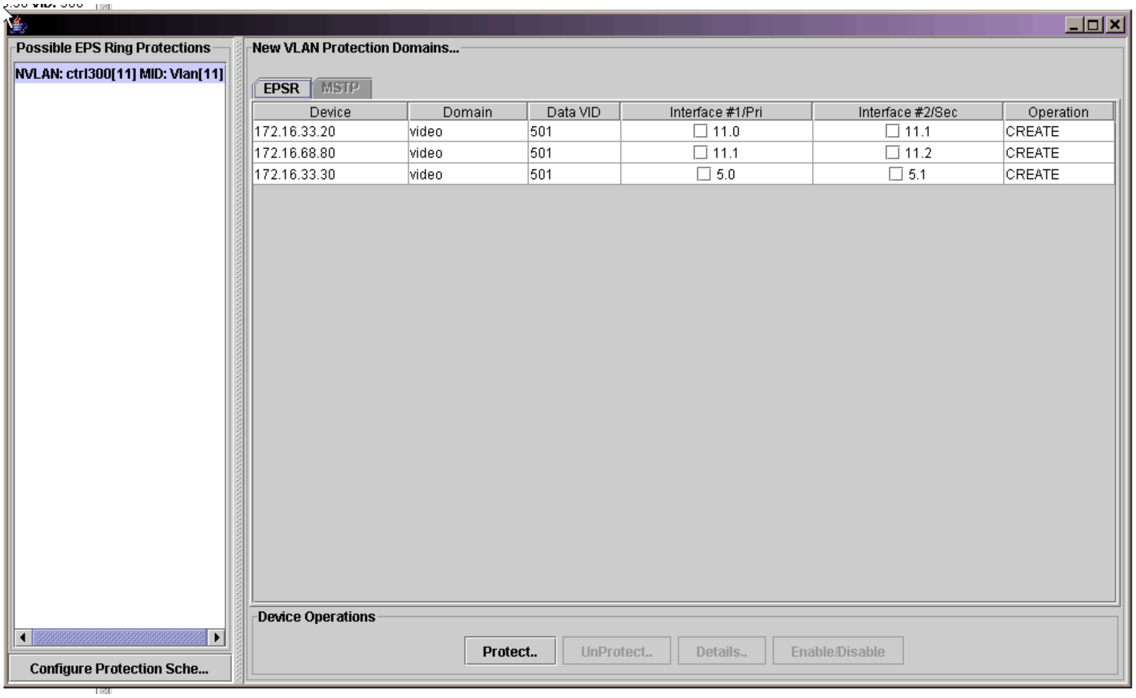
Vlan Name: prot401

```
Vlan Name: The name of the vlan created on the device(s).
VID: The VID that be used for the Data Networked Vlan.


This GUI will create Vlan interface(s) along the path for a selected Control-
Networked VLAN
```

FIGURE 16-55 Creating an EPSR Data Ring by Cloning Control Ring

The user fills in the VID and the Vlan Name. The user clicks on OK, and this brings up the Protection Ring Configuration Panel with all columns filled in, as shown in Figure 16-56.

If more than one control ring could be applied to the data network VLAN, these will appear in the Possible EPS Ring Protections list. The user should select the one that will be used.


Possible EPS Ring Protections
NVLAN: ctrl300[11] MID: Vlan[11]
Configure Protection Sche...
New VLAN Protection Domains...
EPSR
MSTP
Device Operations
Protect..
UnProtect..
Details..
Enable/Disable

Device	Domain	Data VID	Interface #1/Pri	Interface #2/Sec	Operation
172.16.33.20	video	501	□ 11.0	□ 11.1	CREATE
172.16.68.80	video	501	□ 11.1	□ 11.2	CREATE
172.16.33.30	video	501	□ 5.0	□ 5.1	CREATE

FIGURE 16-56 Protection Data Ring Configuration Panel

Finally, the user selects **Configure Protection Scheme**. The Task List window appears as the data ring attributes are applied to the devices. The data ring is now included in the protection domain of the associated control ring.

Table 16-8 lists the fields of the Configure EPS Data Ring panel.

TABLE 16-8 **Fields for the Configure EPS Data Ring Panel**

Option	Purpose
Configure Protection Scheme	Applies (CREATE operation) the EPS data ring attributes (control ring domain, VID, etc.) to the devices listed.
New VLAN Protection Domains... panel	Lists the relevant information for the created data protection ring (No fields are editable) Device: The name that has been given to the device Domain: The domain of the associated EPS control ring Data VID: The VID that will be used to define the VLAN interfaces for the devices Interface #1/Pri: The ports that make up the primary interface Interface #2/Sec: The ports that make up the secondary interface Operation: The next logical operation that can be performed.
Device Operations	Options to perform on the protected data VLAN **Protect** - Will create the protection ring over the domain of the control ring. **Unprotect** - Activated only when the EPS Data Ring has already been created, allows the user to delete the protection domain for the network VLAN. Note that the network VLAN itself is not deleted. Refer to "Unprotect Data Protection Ring" on page 578.

- For **option 2**, an existing Data Networked VLAN is selected to become a Protected Data Network VLAN. The Network VLAN Manager shows the map for the VLAN Interface. The user then selects **Create/Protect EPS Data Ring**, and the Protection Data Ring Configuration Panel appears with the same options as shown in Figure 16-56. Once **Configure Protection Scheme** is selected, the application will complete the data protection ring (and create any additional VLAN Interfaces) as well.
- **Option 3** is similar to Option 2, but since the network data VLAN has already been configured as a ring, completion of the data network VLAN to form a ring by the application is not needed.

16.10.3.2 Unprotect Data Protection Ring

To unprotect an EPS data ring, the user selects the newly created data protection ring and right-clicks **View EPS Data Protection...**This bring up the Configure EPS Data Ring Panel with all of its attributes. The data ring can now be unprotected, using the following strategies:

- The user can choose a port to be deleted from the VLAN interface so that it will not form a loop after it becomes unprotected. Note that the unselected ports are the ones which will be unprotected.
- If the user chooses no ports, this will delete all the VLAN interfaces on **all** the devices.

16.10.4 Configuration Guidelines

The creation of an EPSR configuration should be planned and engineered carefully to ensure that the resulting topology has the desired results. The following notes and warnings that must be taken into account when the EPSR is introduced.

Note: One of the advantages of using the AlliedView NMS GUI (Network VLAN Manager application) is that many of these rules are automatically enforced or allow configuration errors to be easily seen and corrected.

Before configuring an EPSR topology, the following rules must be considered, since they will affect how the EPSR topology will fit into the network and how the network will be affected during the configuration steps:

- The ports used for EPSR are gigabit ethernet ports only.

- EPSR and other protection schemes (STP/RSTP) are mutually exclusive; **ports that use EPSR will have STP disabled**.
- Ensure that a loop is not created while provisioning the protected VLANs (or ensure that there is no traffic on the protected VLANs until the VLAN is added to the EPSR domain).
- Provisioning can be done in two ways:
  - Pre-provision - The AlliedView NMS allows the administrator to pre-provision the cards, links, and network VLANs. This does not affect current traffic since the hardware does not actually exist. Once the configuration is tested (GUI maps are checked), the hardware can be installed, links actually connected between devices, and the states of the devices will change so they are ready to pass traffic as pre-provisioned.
  - Post-provision - All the hardware is already provisioned, allowing the administrator to provision the EPSR control ring, add existing traffic-live network VLANS, and protect them.

Keeping in mind the rules above, the administrator should plan out the following:

- The devices, ports, and links between the ports that will be included in the EPSR configuration.
- The name and number of the control VLAN.
- The name of the domain that will include the master and transit devices, and for the master device which interfaces (ports) will be initially primary and secondary.
- The name and number of the protected VLAN(s) to be added to the EPSR domain.

16.10.5 Example Scenario

Figure 16-57 shows the physical/logical configuration for the example scenario.

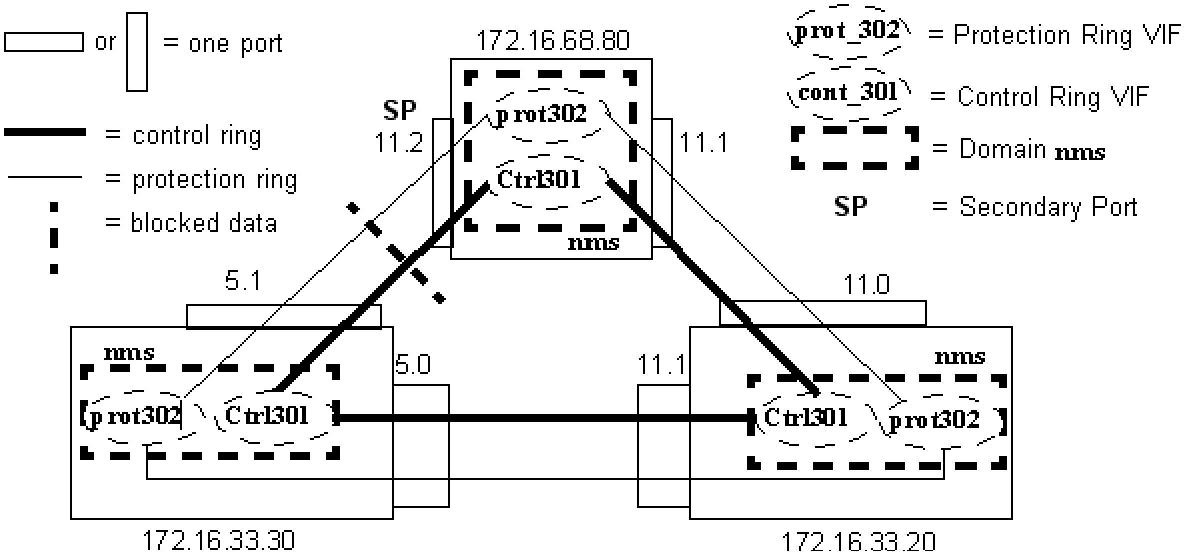
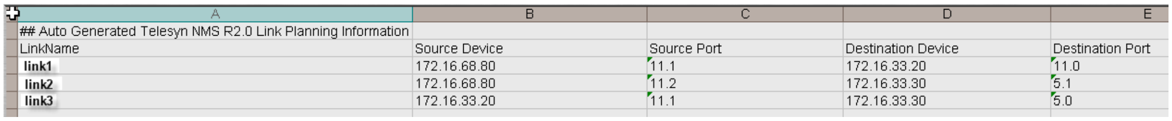


FIGURE 16-57 Example Ring Topology - Physical/Logical

16.10.5.1 Set up the Links Between the Ports

Using the NMS physical link feature, create a spreadsheet that includes the links (with devices and ports) that will be included in the EPSR configuration. Load the spreadsheet so that the physical links in Figure 16-58 are known to the AlliedView NMS. The following figure shows an example spreadsheet. Refer to "Importing Physical Link Configurations" on page 546 for creating and importing a spreadsheet.

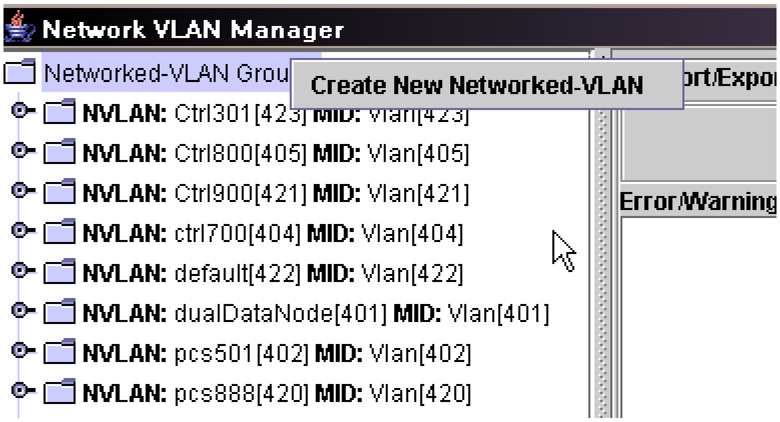


A	B	C	D	E
## Auto Generated Telesyn NMS R2.0 Link Planning Information				
LinkName	Source Device	Source Port	Destination Device	Destination Port
link1	172.16.68.80	11.1	172.16.33.20	11.0
link2	172.16.68.80	11.2	172.16.33.30	5.1
link3	172.16.33.20	11.1	172.16.33.30	5.0

FIGURE 16-58 Example Spreadsheet

16.10.5.2 Create a Closed Network VLAN that will become the Control Ring

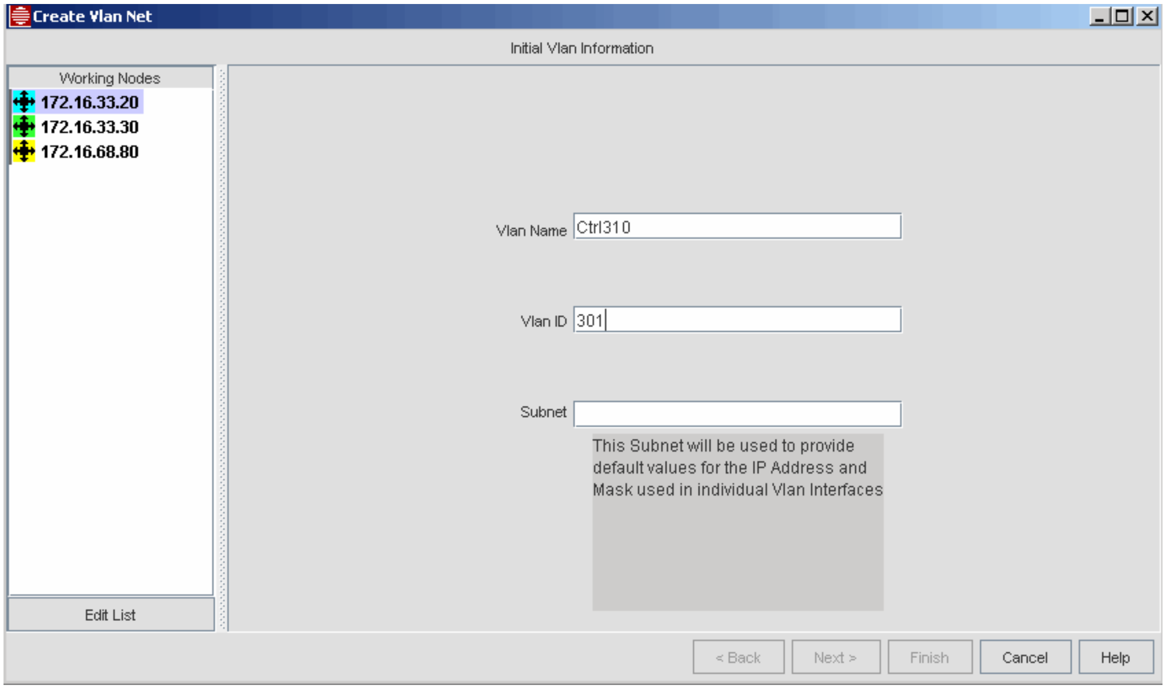
Using the Network VLAN Manager, create a new networked-VLAN, as shown in Figure 16-59



NVLAN: Ctrl301[423] MID: Vlan[423]
NVLAN: Ctrl800[405] MID: Vlan[405]
NVLAN: Ctrl900[421] MID: Vlan[421]
NVLAN: ctrl700[404] MID: Vlan[404]
NVLAN: default[422] MID: Vlan[422]
NVLAN: dualDataNode[401] MID: Vlan[401]
NVLAN: pcs501[402] MID: Vlan[402]
NVLAN: pcs888[420] MID: Vlan[420]

FIGURE 16-59 Creating a Network-VLAN to Become a Control Ring

In the resulting Initial Vlan Information window, fill in the Control VLAN values, as shown in Figure 16-60.



172.16.33.20
172.16.33.30
172.16.68.80

Vlan Name: Ctrl310

Vlan ID: 301

Subnet:

This Subnet will be used to provide default values for the IP Address and Mask used in individual Vlan Interfaces

FIGURE 16-60 Data filling Control VLAN Values

A looped network VLAN for the devices has now been created, and so can be configured as the control ring.

16.10.5.3 Configure the Control Ring

With the network VLAN (Ctrl301) created, use the Network VLAN Manager to configure the Control Ring, as shown in Figure 16-61. Figure 16-62 warns the user about disconnecting unprotected Network VLANs and that STP will be disabled.

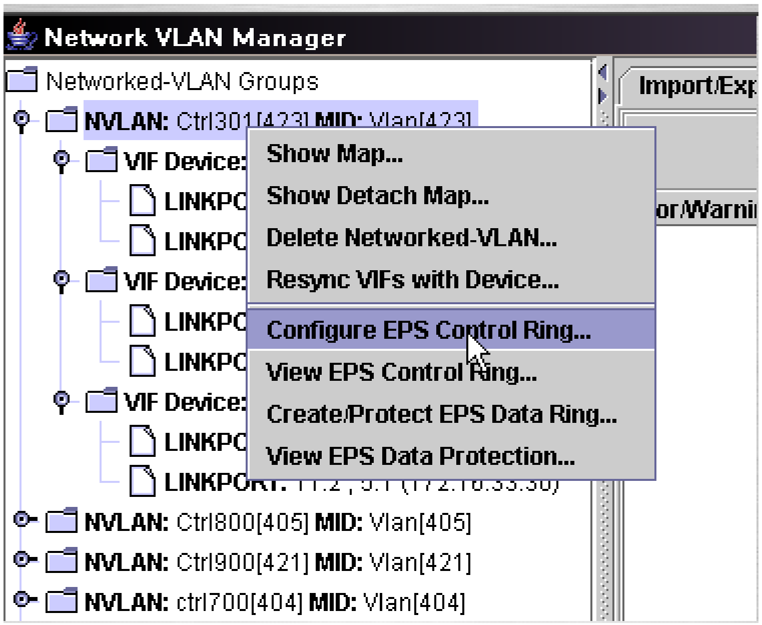
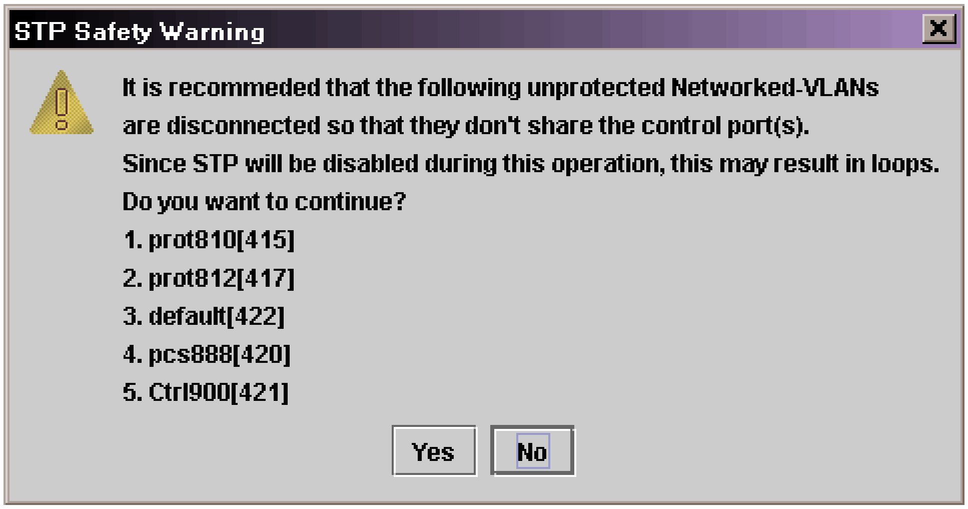

Network VLAN Manager
Networked-VLAN Groups
NVLAN: Ctrl301[423] MID: Vlan[423]
VIF Device:
LINKPO
LINKPO
VIF Device:
LINKPO
LINKPO
VIF Device:
LINKPO
LINKPORT: 11.2 ; 5.1 (172.16.33.30)
NVLAN: Ctrl800[405] MID: Vlan[405]
NVLAN: Ctrl900[421] MID: Vlan[421]
NVLAN: ctrl700[404] MID: Vlan[404]
Import/Exp
or/Warni
Show Map...
Show Detach Map...
Delete Networked-VLAN...
Resync VIFs with Device...
Configure EPS Control Ring...
View EPS Control Ring...
Create/Protect EPS Data Ring...
View EPS Data Protection...

FIGURE 16-61 Configuring Network VLAN as Control Ring

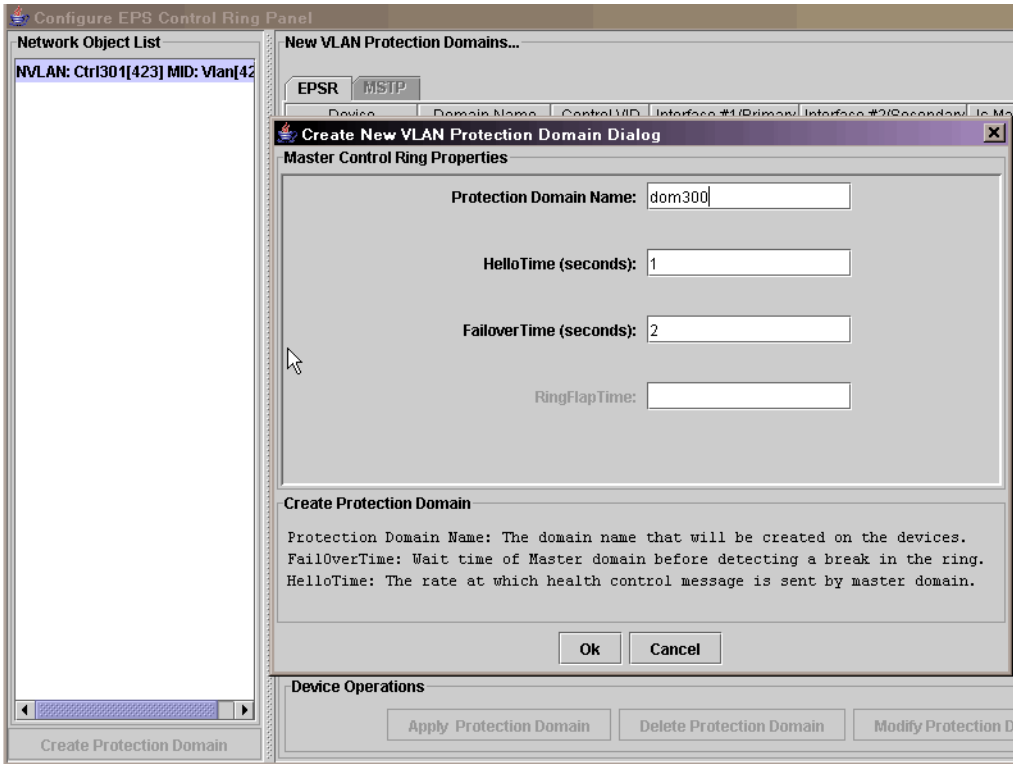


It is recommeded that the following unprotected Networked-VLANs are disconnected so that they don't share the control port(s).
Since STP will be disabled during this operation, this may result in loops.
Do you want to continue?

1. prot810[415]
2. prot812[417]
3. default[422]
4. pcs888[420]
5. Ctrl900[421]

FIGURE 16-62 STP Safety Warning

Clicking on **Yes** brings up the **Create New VLAN Protection Domain** Dialog. Fill in the domain (dom300) and adjust the protocol values if necessary, as shown in Figure 16-63.



Protection Domain Name: dom300

HelloTime (seconds): 1

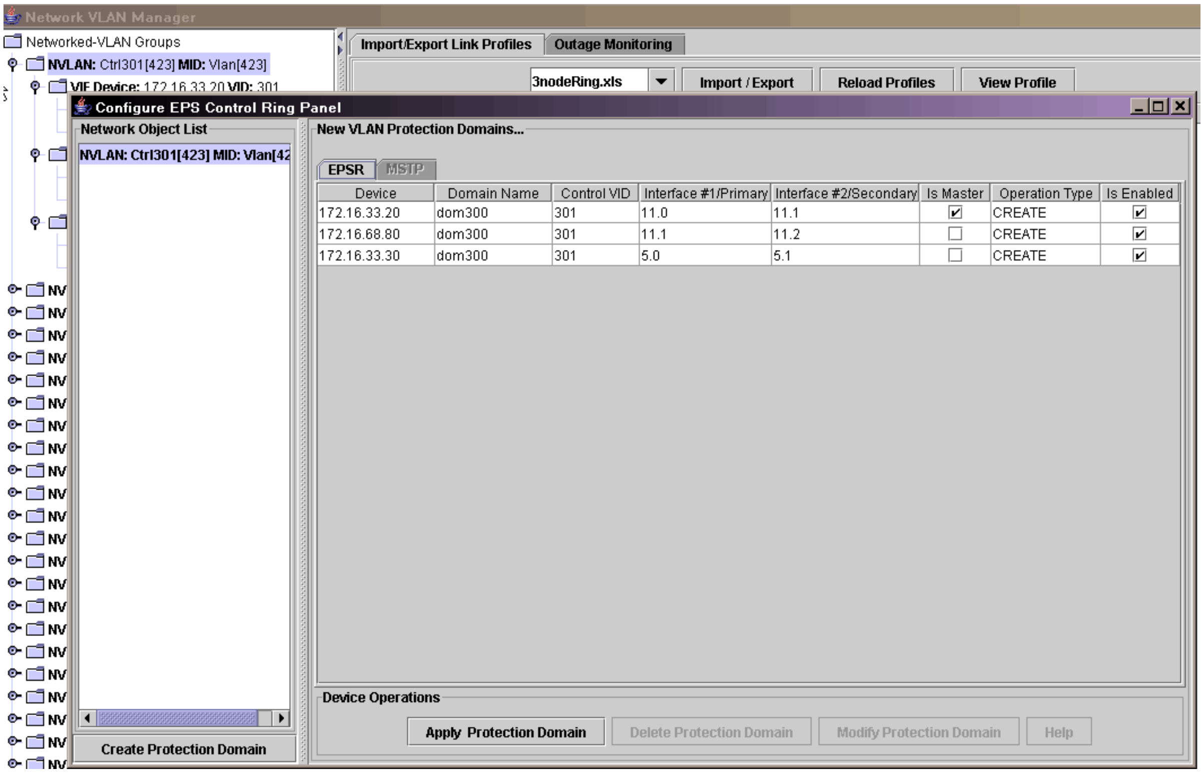
FailoverTime (seconds): 2

RingFlapTime:

```
Protection Domain Name: The domain name that will be created on the devices.
FailOverTime: Wait time of Master domain before detecting a break in the ring.
HelloTime: The rate at which health control message is sent by master domain.
```

FIGURE 16-63 Creating Control VLAN Domain

Clicking on **OK**, the configuration that will be created is shown in Figure 16-64.

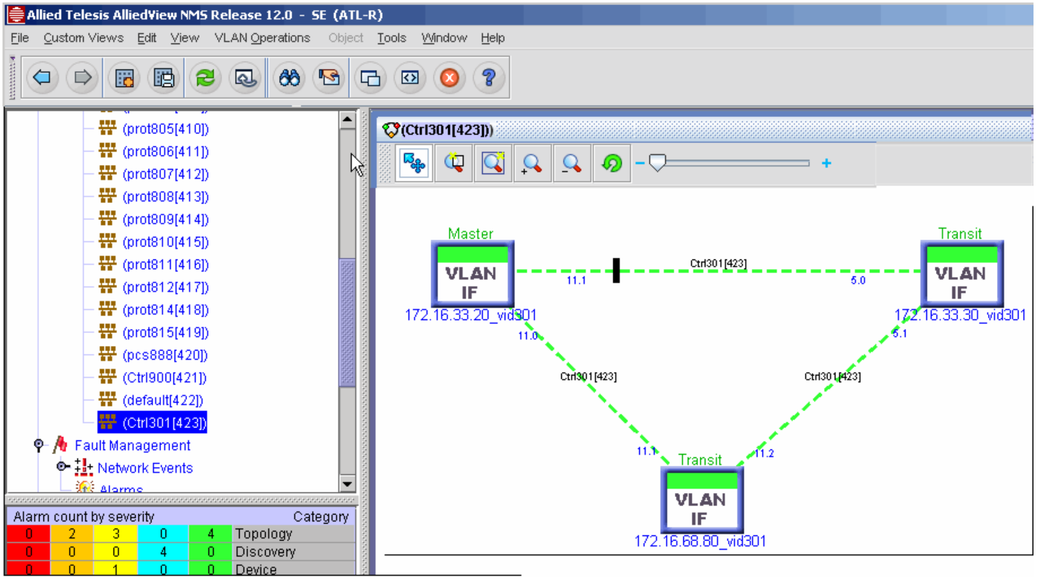


Device	Domain Name	Control VID	Interface #1/Primary	Interface #2/Secondary	Is Master	Operation Type	Is Enabled
172.16.33.20	dom300	301	11.0	11.1	☑	CREATE	☑
172.16.68.80	dom300	301	11.1	11.2	☐	CREATE	☑
172.16.33.30	dom300	301	5.0	5.1	☐	CREATE	☑

FIGURE 16-64 Configuration for Control Ring Panel

Clicking on **Create Protection Domain** invokes the Task Manager, which lists the task being performed for each device. Once the tasks complete successfully, click on the Ctrl301 VLAN IF and the map shows graphically how the control VLAN is configured, as shown in Figure 16-65.

Refer back to Figure 16-57 to see how the GUI matches the planned configuration.



Alarm count by severity					Category
0	2	3	0	4	Topology
0	0	0	4	0	Discovery
0	0	1	0	0	Device

FIGURE 16-65 GUI of Control Ring

16.10.5.4 Create a Data Ring

A preferred way to create a Data Ring is to clone the just created Control Ring. In the Network VLAN Manager, select the Control Ring Network VLAN (Ctrl301) and right click on Create/Protect EPS Data RIng, as shown in Figure 16-66.

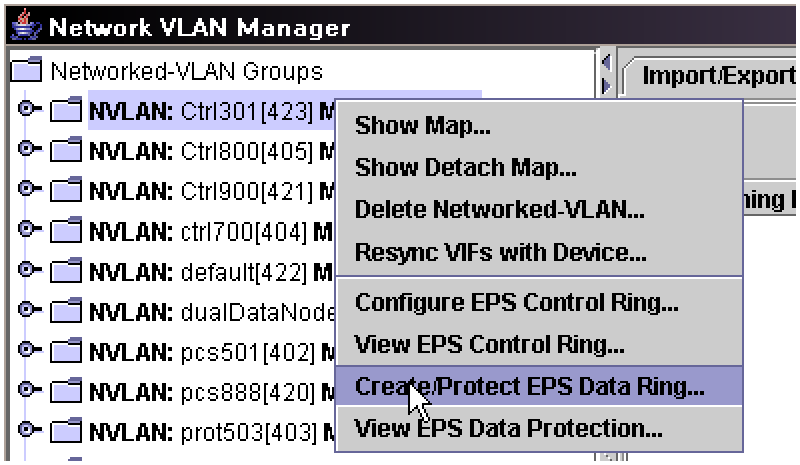
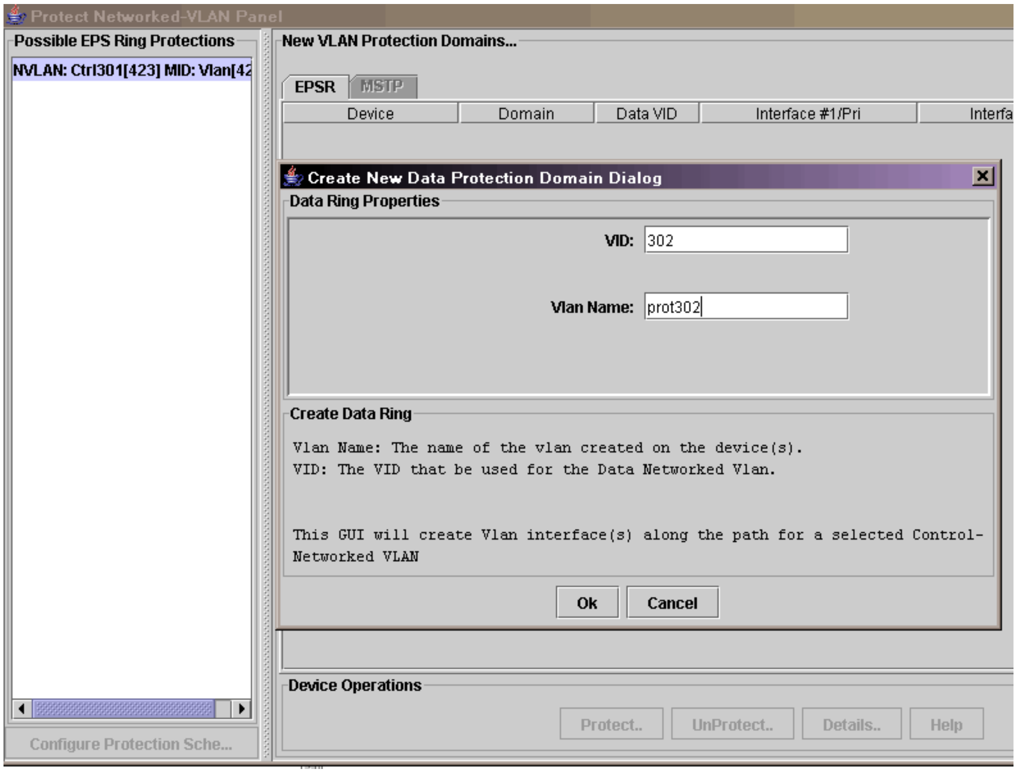


FIGURE 16-66 Creating a Data Ring from an Existing Control Ring

The Create New Data Protection Ring Dialog appears, as shown in Figure 16-67.


Protect Networked-VLAN Panel
Possible EPS Ring Protections
NVLAN: Ctrl301[423] MID: Vlan[42
Configure Protection Sche...
New VLAN Protection Domains...
EPSR
MSTP
Device
Domain
Data VID
Interface #1/Pri
Interfa
Create New Data Protection Domain Dialog
Data Ring Properties
Create Data Ring
Ok
Cancel
Device Operations
Protect..
UnProtect..
Details..
Help

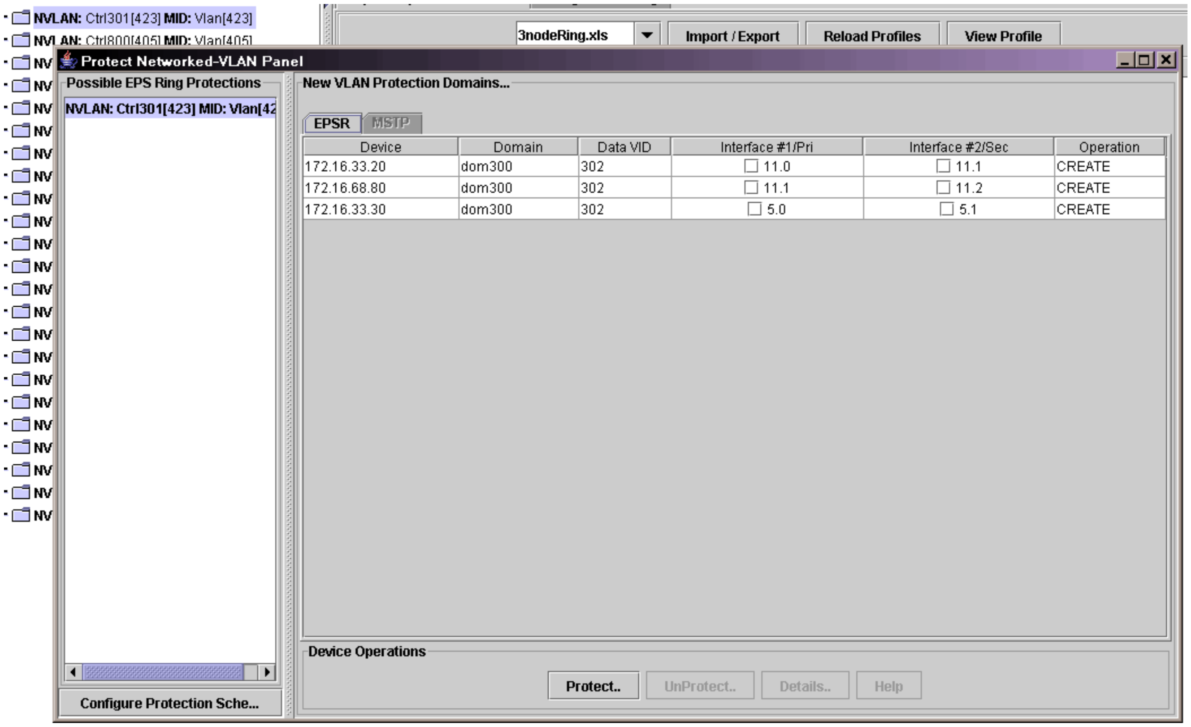
VID: 302

Vlan Name: prot302

```
Vlan Name: The name of the vlan created on the device(s).
VID: The VID that be used for the Data Networked Vlan.


This GUI will create Vlan interface(s) along the path for a selected Control-
Networked VLAN
```

FIGURE 16-67 Creating the Protection Ring Network VLAN (from the Control Ring)

Input the VID (always a number) and Vlan Name and click on **OK**. The configuration that results from this is shown in Figure 16-68.


NVLAN: Ctrl301[423] MID: Vlan[423]
NVLAN: Ctrl800[405] MID: Vlan[405]
3nodeRing.xls
Import / Export
Reload Profiles
View Profile
Protect Networked-VLAN Panel
Possible EPS Ring Protections
NVLAN: Ctrl301[423] MID: Vlan[42
New VLAN Protection Domains...
EPSR
MSTP
Device Operations
Protect..
UnProtect..
Details..
Help
Configure Protection Sche...

Device	Domain	Data VID	Interface #1/Pri	Interface #2/Sec	Operation
172.16.33.20	dom300	302	□ 11.0	□ 11.1	CREATE
172.16.68.80	dom300	302	□ 11.1	□ 11.2	CREATE
172.16.33.30	dom300	302	□ 5.0	□ 5.1	CREATE

FIGURE 16-68 Configuration for Data Protection Ring

Clicking on **Configure Protection Scheme** brings up the Task window to perform the configuration for each device. Once done, selecting the VLAN IF for prot302 shows the GUI, in Figure 16-69. Compare this to Figure 16-57.

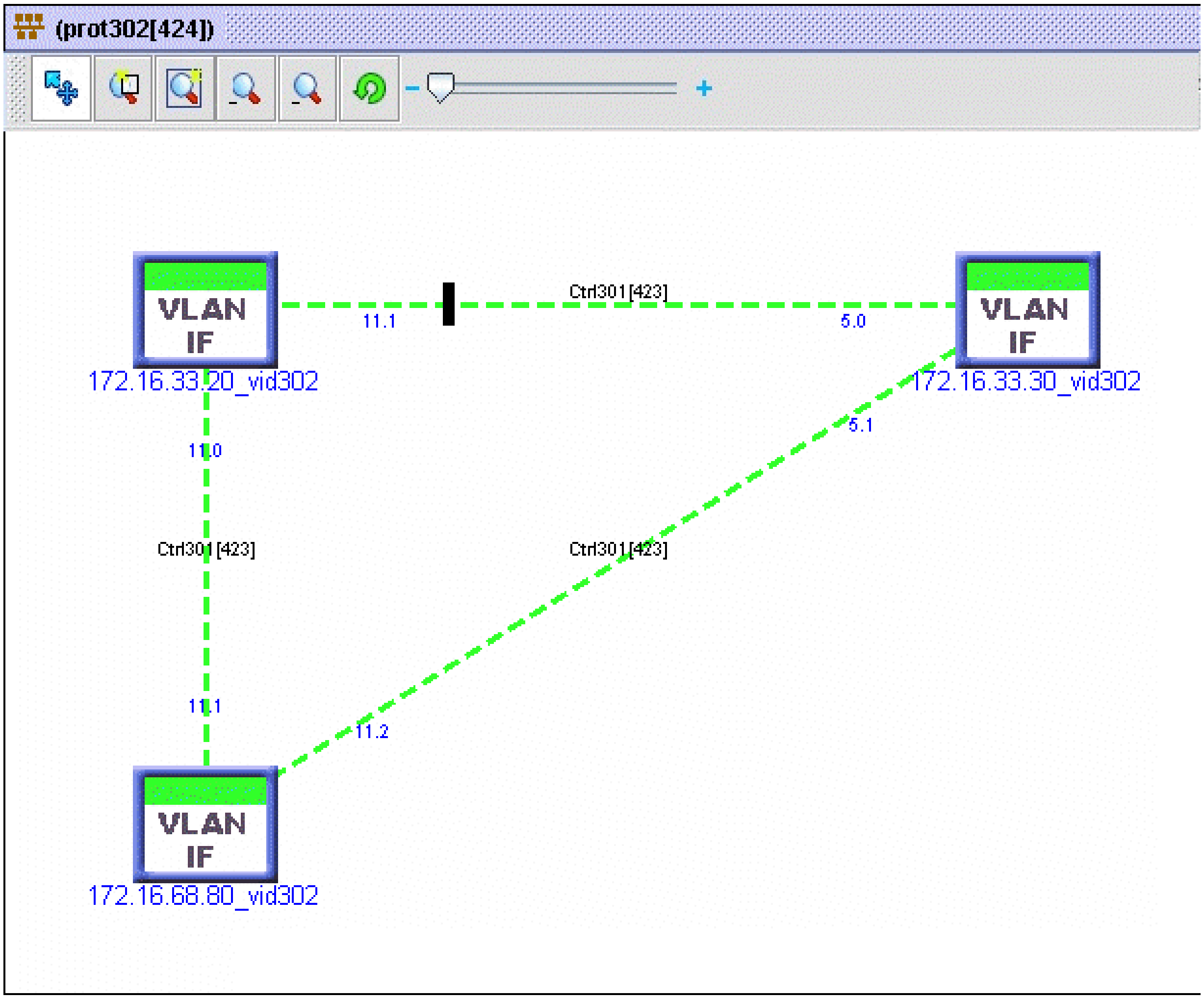


FIGURE 16-69 GUI for Configured Protection Data Ring

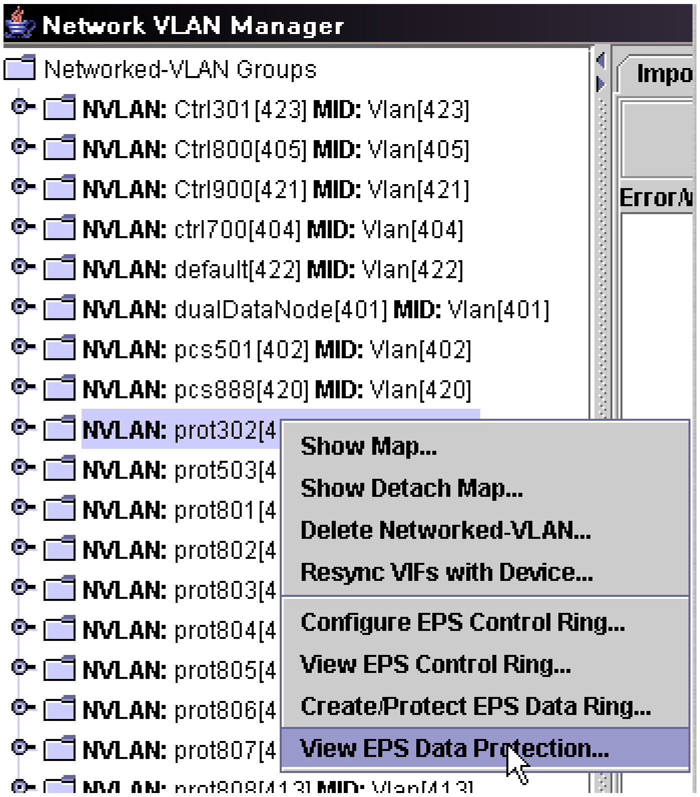
16.10.5.5 Reconfigure the Control and Data Rings

Now that the Control Ring and Data Ring are configured, another device may need to be added to the configuration. Performing this involves combining many of the network services tasks, summarized as follows:

- Reconfigure the links between two current devices and the new device.
  - Delete the link between the current devices.
  - Add the links between the new device and the two current devices.
  - Extend the VLANs to include the new device
- Associate the Control Ring with the extended VLAN Interface
  - Select the VIF to configure the Control Ring
  - Use the same domain name, and extend to the new device.
- Extend the Data Ring
  - Delete the Network VLAN of the Data Ring
  - Reclone the Data Ring from the Control Ring

16.10.5.6 Modify/Unprotect the Data Ring

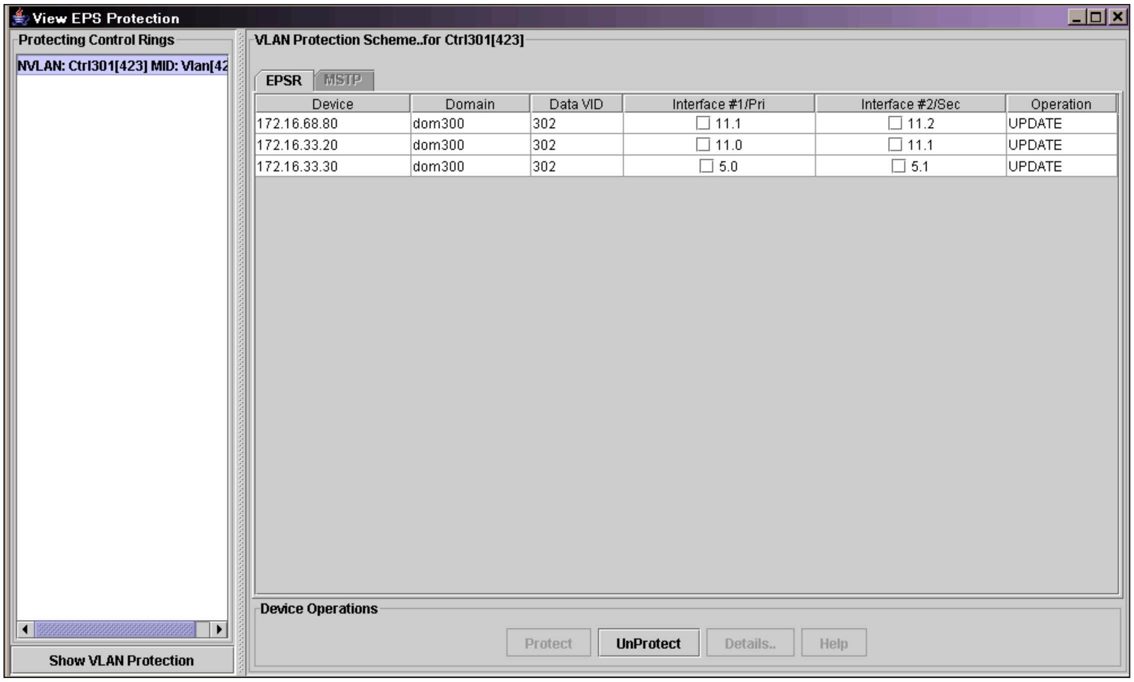
The configured Data Ring can be modified if necessary. Select the Data Protection Ring and select View EPS Data Protection, as shown in Figure 16-69.


Network VLAN Manager
Impo
Error/
Show Map...
Show Detach Map...
Delete Networked-VLAN...
Resync VIFs with Device...
Configure EPS Control Ring...
View EPS Control Ring...
Create/Protect EPS Data Ring...
View EPS Data Protection...

Networked-VLAN Groups
NVLAN: Ctrl301[423] **MID:** Vlan[423]
NVLAN: Ctrl800[405] **MID:** Vlan[405]
NVLAN: Ctrl900[421] **MID:** Vlan[421]
NVLAN: ctrl700[404] **MID:** Vlan[404]
NVLAN: default[422] **MID:** Vlan[422]
NVLAN: dualDataNode[401] **MID:** Vlan[401]
NVLAN: pcs501[402] **MID:** Vlan[402]
NVLAN: pcs888[420] **MID:** Vlan[420]
NVLAN: prot302[4
NVLAN: prot503[4
NVLAN: prot801[4
NVLAN: prot802[4
NVLAN: prot803[4
NVLAN: prot804[4
NVLAN: prot805[4
NVLAN: prot806[4
NVLAN: prot807[4
NVLAN: prot808[413] **MID:** Vlan[413]

FIGURE 16-70 View Data Protection Ring

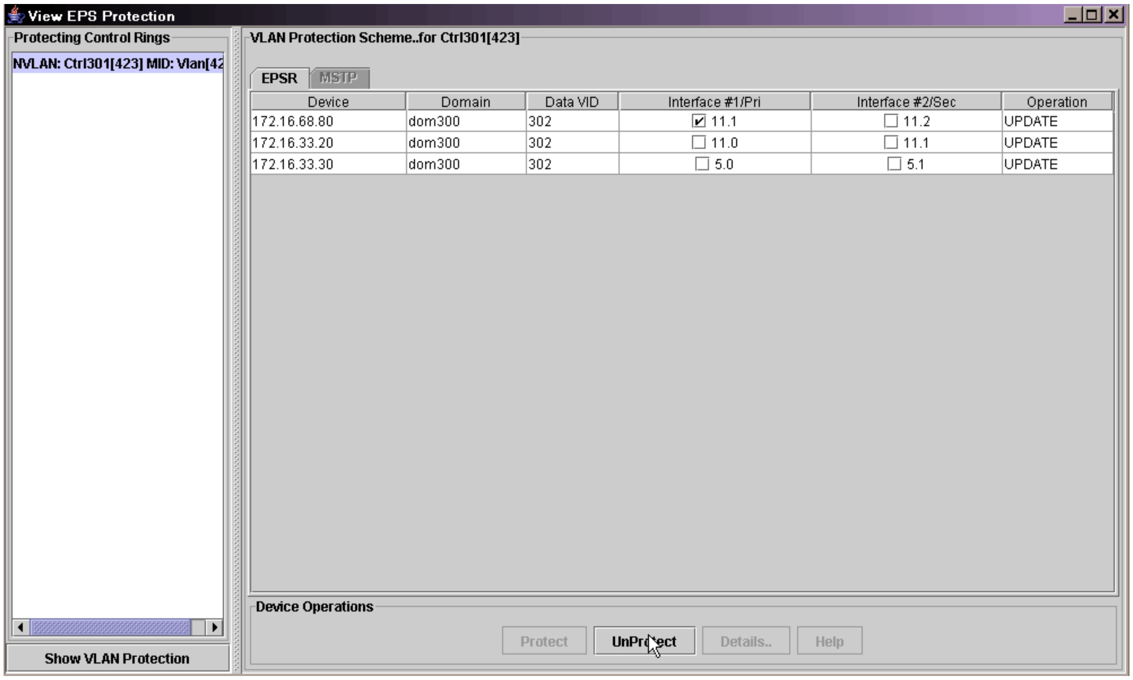
The VLAN Protection Scheme panel appears, showing the Domain, Data VIDs, etc, for the Data Protection Network VLAN, as shown in Figure 16-71.



Device	Domain	Data VID	Interface #1/Pri	Interface #2/Sec	Operation
172.16.68.80	dom300	302	□ 11.1	□ 11.2	UPDATE
172.16.33.20	dom300	302	□ 11.0	□ 11.1	UPDATE
172.16.33.30	dom300	302	□ 5.0	□ 5.1	UPDATE

FIGURE 16-71 View Protection Ring Configuration

At this point the user could select one of the Primary Interfaces and click on Unprotect, as shown in Figure 16-72.



Device	Domain	Data VID	Interface #1/Pri	Interface #2/Sec	Operation
172.16.68.80	dom300	302	☑ 11.1	□ 11.2	UPDATE
172.16.33.20	dom300	302	□ 11.0	□ 11.1	UPDATE
172.16.33.30	dom300	302	□ 5.0	□ 5.1	UPDATE

FIGURE 16-72 Selecting an Interface on a Device and Unprotect

After the Task Details Window had opened and closed, the user could select the VLAN IF and see that the Network VLAN no longer had a protection scheme, as shown in Figure 16-73. Since 11.1 of 68.80 is selected, the link will be retained (port will not be deleted).

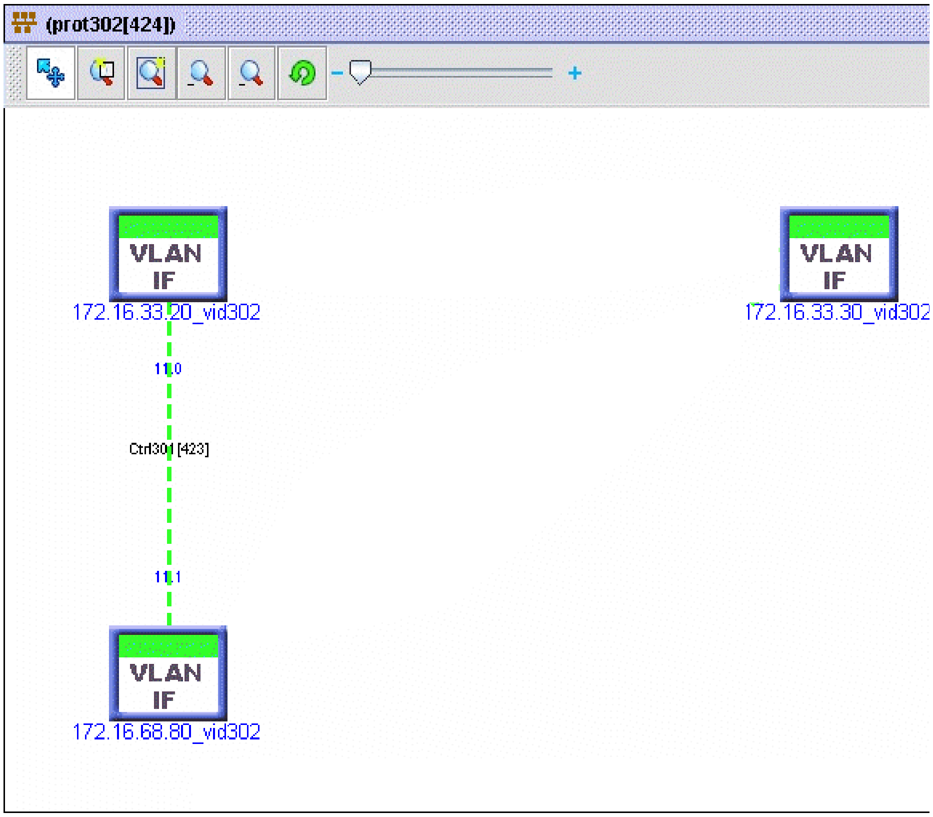


FIGURE 16-73 GUI for Network VLAN no Longer with a Protection Scheme

16.10.6 Troubleshooting the EPSR Configuration

Using the AlliedView NMS GUI allows the network administrator to more easily understand and resolve the following maintenance scenarios:

- The EPS Control and Data rings are not configured properly and so cannot provide the protection service as described in "Overview of EPSR Topology" on page 567
- A path for the protected data VLAN has broken, and the secondary path has been activated.
- Both the primary and secondary paths for a device are broken, with a loss data service to and from that device.

16.10.6.1 Errors in EPSR Configuration

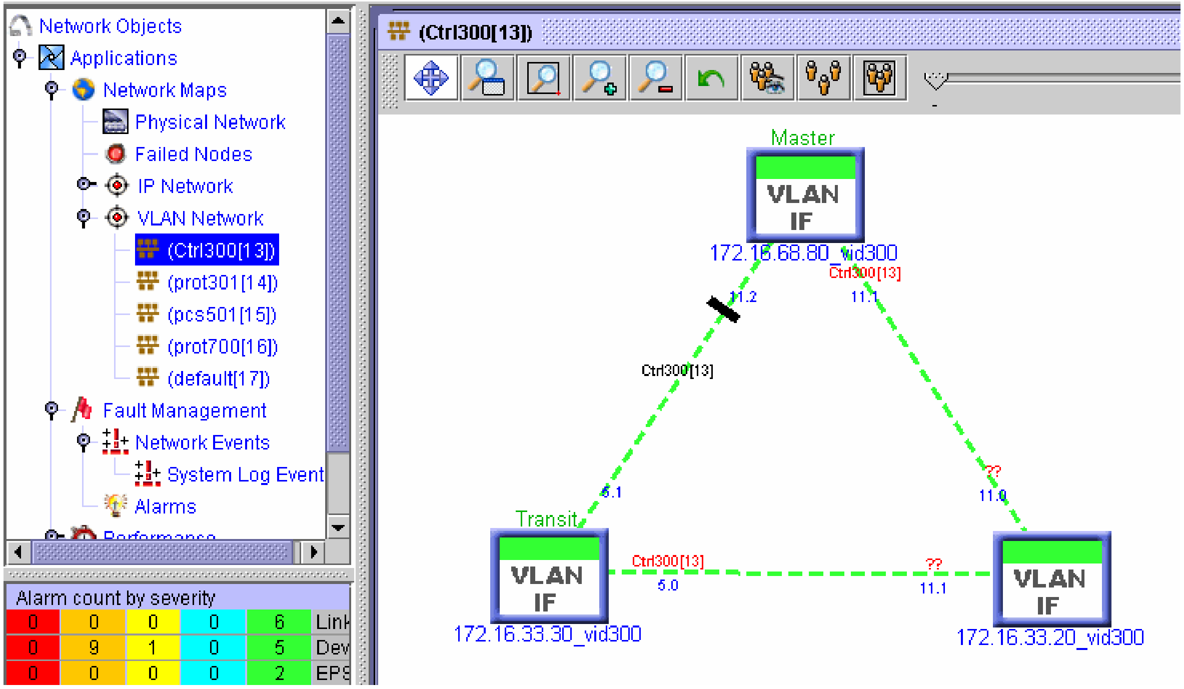
By using the AlliedView NMS GUI, the administrator can usually avoid most configuration errors and produce a control ring and associated data rings that follow the configuration guidelines listed in "Configuration Guidelines" on page 578. However, if there are configuration errors (usually done by configuring each device separately through the command interface), the GUI allows the user to easily spot the configuration fault and correct it.

Common EPSR configuration errors can be grouped as follows:

- The protection VLAN is actually unprotected on a device:
  - The protected VLAN interface is not part of the domain with the control VLAN interface
  - The EPSR domain is part of a different control ring.
- The control VLAN is not configured completely/properly
  - There are multiple Masters or no Masters.

- The device is not part of the domain (there are no Master/Transit indicators on the VLAN Interfaces.
- There is an incomplete loop (usually a missing link or device.

In Figure 16-74, a control ring has been configured following the example in Figure 16-57. The .80 device is the master node and the .30 node is a transit node and both are configured (and connected) with the Ctrl300 as the network VLAN. The .20 device is also connected to the ring but is not protected by the Control VLAN Ctrl300. Note that these Ctrl300 labels are in red. Moreover, there are question marks in red on the links coming form the ports. Finally, note that the .20 device has no transit label above it.

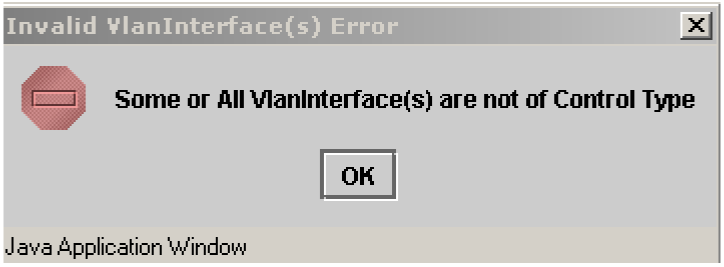


Alarm count by severity

0	0	0	0	6	Link
0	9	1	0	5	Dev
0	0	0	0	2	EPS

FIGURE 16-74 Misconfigured Control Ring

To query this configuration, the user can right click on the .20 device and select **View EPS Control Ring**. The following message appears, as shown below.

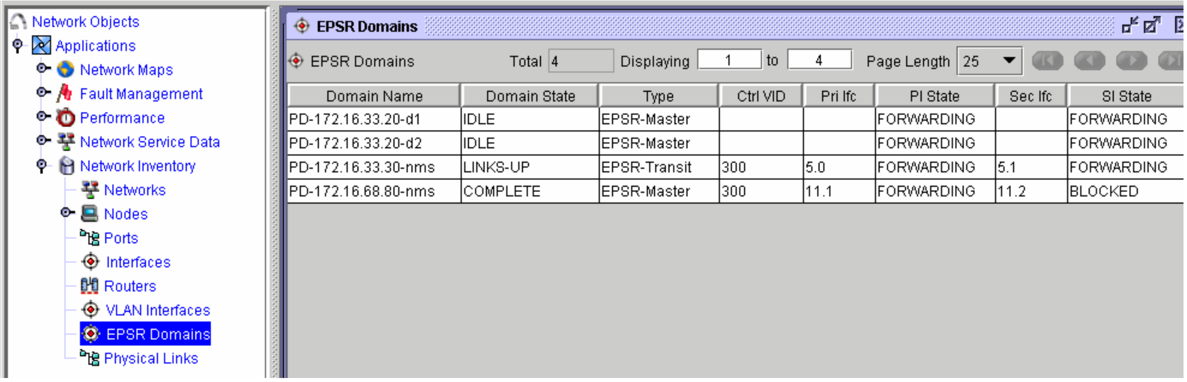


Invalid VlanInterface(s) Error

Some or All VlanInterface(s) are not of Control Type

FIGURE 16-75 Error Message for Misconfigured Control Ring

To view the overall attributes of the EPSR configurations, go to Network Inventory and select EPSR Domains, as shown in the following figure.



Domain Name	Domain State	Type	Ctrl VID	Pri Ifc	PI State	Sec Ifc	SI State
PD-172.16.33.20-d1	IDLE	EPSR-Master			FORWARDING		FORWARDING
PD-172.16.33.20-d2	IDLE	EPSR-Master			FORWARDING		FORWARDING
PD-172.16.33.30-nms	LINKS-UP	EPSR-Transit	300	5.0	FORWARDING	5.1	FORWARDING
PD-172.16.68.80-nms	COMPLETE	EPSR-Master	300	11.1	FORWARDING	11.2	BLOCKED

FIGURE 16-76 EPSR Domains table

Note that the domain name nms is not included for the .20 device for the Ctrl VID 300. Since the links and VLAN interface do exist (according to the GUI maps), the problem must be that the .20 device is not protected by any EPSR Control ring and is not part of a domain.

To resolve this problem, the user can bring up the VLAN Interfaces on .20 device (in this case the VID: 300) and select **Configure EPS Control Ring** ...as shown below. This allows the user to associate the VLAN Interface with the domain used by the Control VLAN.

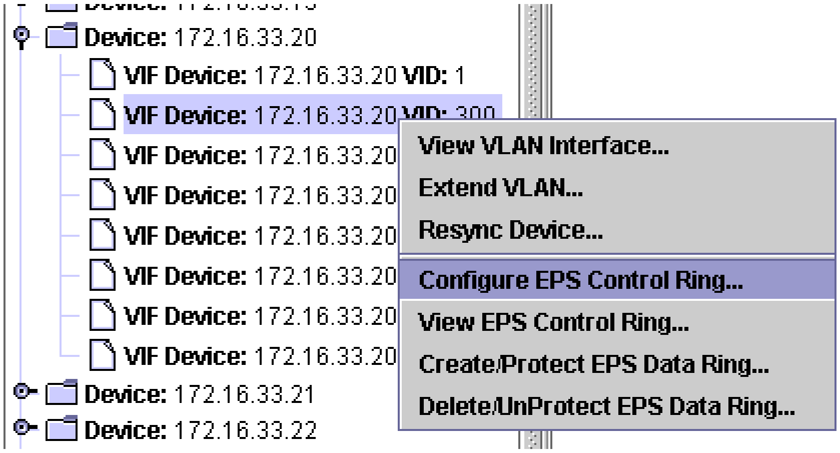


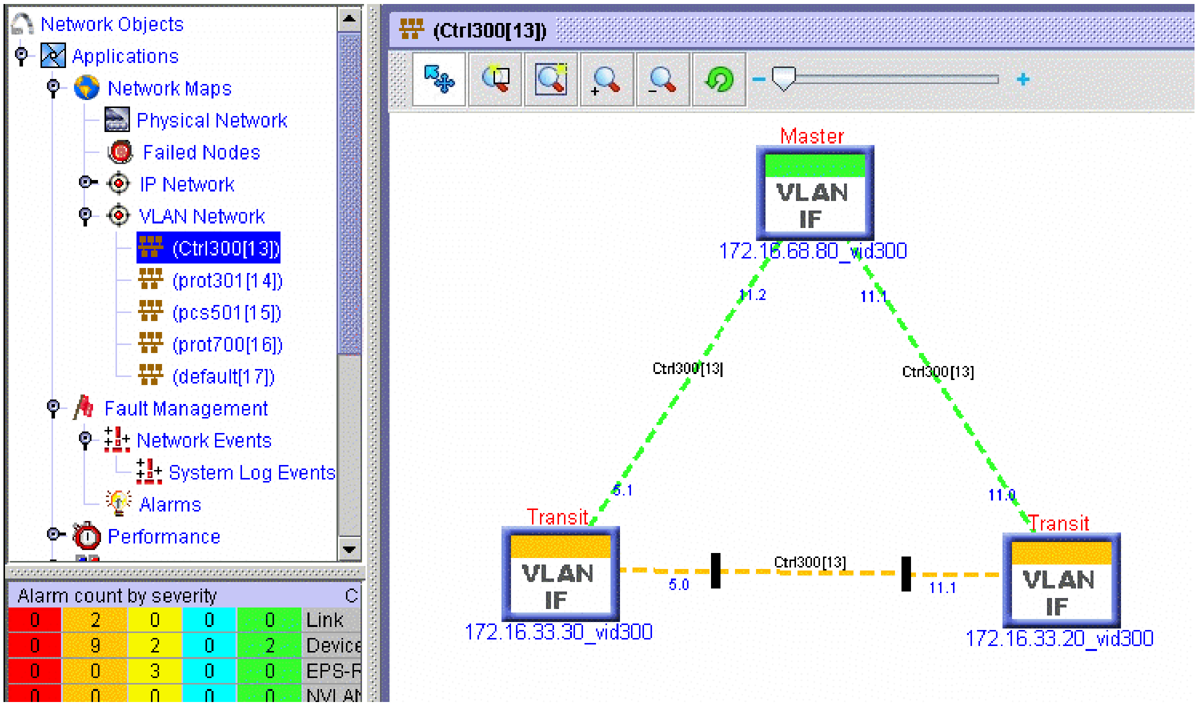
FIGURE 16-77 Control Ring Misconfiguration

16.10.6.2 EPSR Activated (SP Port Now Used for Data Flow)

When any link in the ring is broken, except the link connected to the master's secondary port, the secondary port link is unblocked so data can travel on the alternate path. Details of what is happening to the control messaging are explained in the *Software Reference for iMAP Series Switches*. At the AlliedView NMS, there are several windows that show pictorially what is happening.

Note: The following figures assume that port 11.1 on the .20 device has been disconnected or disabled.

- Control Ring - The following figure shows that the link between the .20 and .30 device is now blocked. The link between .30 and .80, which was previously blocked, has now been opened so that traffic that used to go from .30 to .20 and then to .80 is now going directly to the .20. Moreover, the Master and Transit labels are now red.

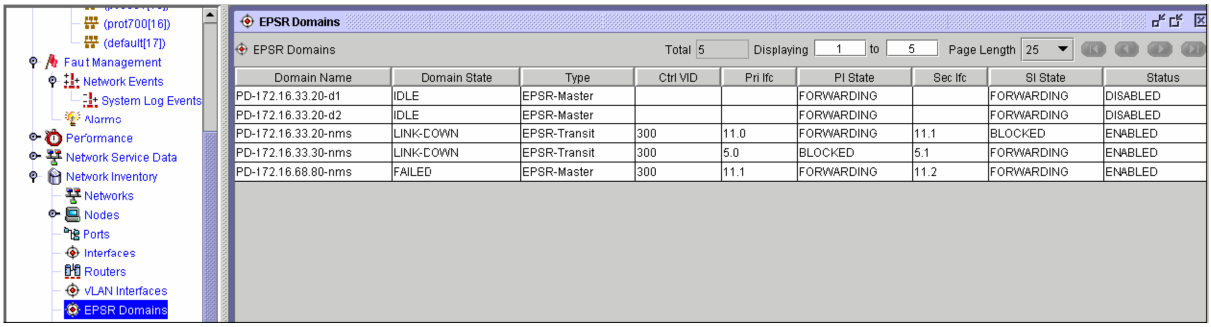


Alarm count by severity C

0	2	0	0	0	Link
0	9	2	0	2	Device
0	0	3	0	0	EPS-F
0	0	0	0	0	NVLAN

FIGURE 16-78 GUI when EPSR Activated

- Network Inventory - The table now includes the LINK DOWN and FAILED states for domain nms and the changed FORWARDING and BLOCKING states that reflect the VLAN map GUI.



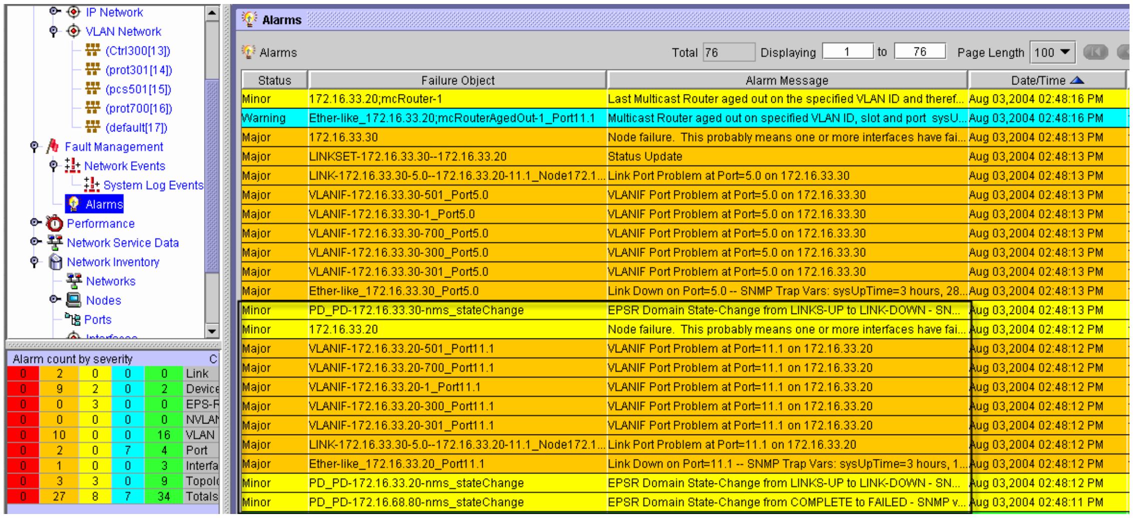
EPSR Domains

EPSR Domains Total 5 Displaying 1 to 5 Page Length 25

Domain Name	Domain State	Type	Ctrl VID	Pri Ifc	PI State	Sec Ifc	SI State	Status
PD-172.16.33.20-d1	IDLE	EPSR-Master			FORWARDING		FORWARDING	DISABLED
PD-172.16.33.20-d2	IDLE	EPSR-Master			FORWARDING		FORWARDING	DISABLED
PD-172.16.33.20-nms	LINK-DOWN	EPSR-Transit	300	11.0	FORWARDING	11.1	BLOCKED	ENABLED
PD-172.16.33.30-nms	LINK-DOWN	EPSR-Transit	300	5.0	BLOCKED	5.1	FORWARDING	ENABLED
PD-172.16.68.80-nms	FAILED	EPSR-Master	300	11.1	FORWARDING	11.2	FORWARDING	ENABLED

FIGURE 16-79 EPSR with FAILED States

- Alarms - Viewing the alarms shows all of the associated alarms, as highlighted below.



Alarm count by severity C

0	2	0	0	0	Link
0	9	2	0	2	Device
0	0	3	0	0	EPS-F
0	0	0	0	0	NVLAI
0	10	0	0	16	VLAN
0	2	0	7	4	Port
0	1	0	0	3	Interfa
0	3	3	0	9	Topolo
0	27	8	7	34	Totals

Alarms

Total 76 Displaying 1 to 76 Page Length 100

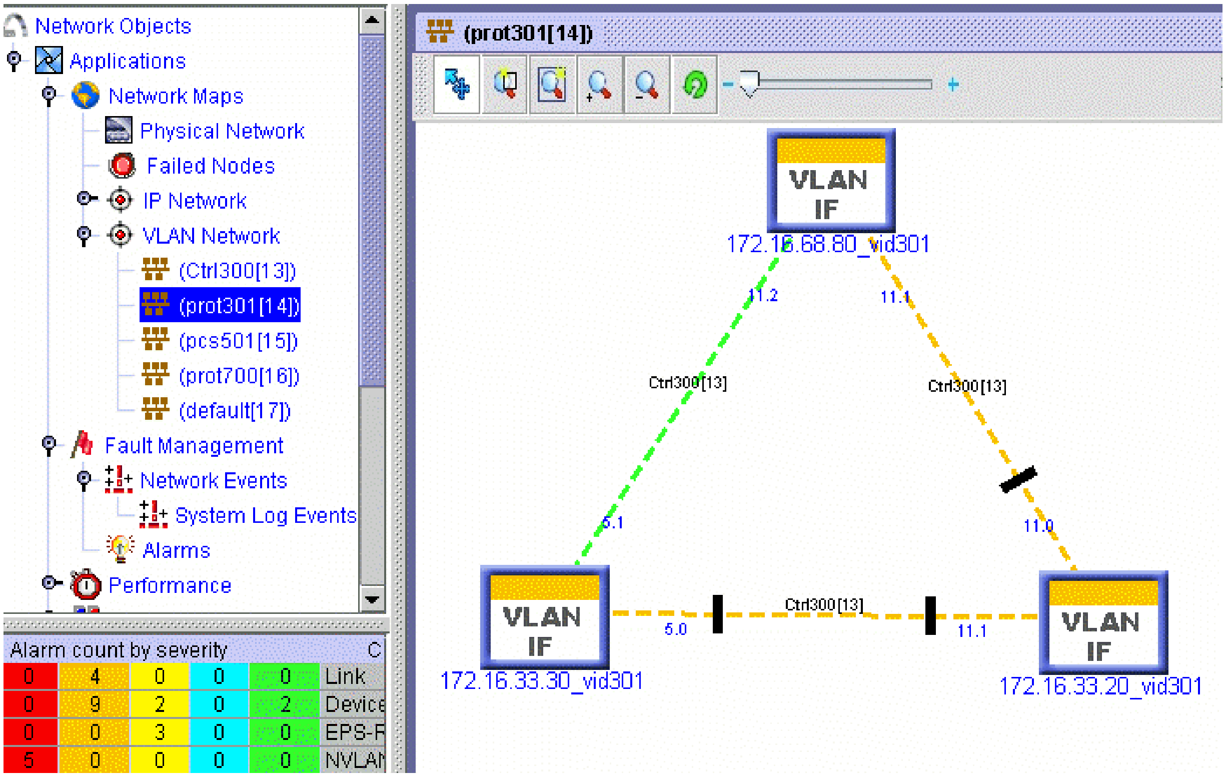
Status	Failure Object	Alarm Message	Date/Time
Minor	172.16.33.20;mcRouter-1	Last Multicast Router aged out on the specified VLAN ID and theref...	Aug 03,2004 02:48:16 PM
Warning	Ether-like_172.16.33.20;mcRouterAgedOut-1_Port11.1	Multicast Router aged out on specified VLAN ID, slot and port sysU...	Aug 03,2004 02:48:16 PM
Major	172.16.33.30	Node failure. This probably means one or more interfaces have fai...	Aug 03,2004 02:48:13 PM
Major	LINKSET-172.16.33.30--172.16.33.20	Status Update	Aug 03,2004 02:48:13 PM
Major	LINK-172.16.33.30-5.0--172.16.33.20-11.1_Node172.1...	Link Port Problem at Port=5.0 on 172.16.33.30	Aug 03,2004 02:48:13 PM
Major	VLANIF-172.16.33.30-501_Port5.0	VLANIF Port Problem at Port=5.0 on 172.16.33.30	Aug 03,2004 02:48:13 PM
Major	VLANIF-172.16.33.30-1_Port5.0	VLANIF Port Problem at Port=5.0 on 172.16.33.30	Aug 03,2004 02:48:13 PM
Major	VLANIF-172.16.33.30-700_Port5.0	VLANIF Port Problem at Port=5.0 on 172.16.33.30	Aug 03,2004 02:48:13 PM
Major	VLANIF-172.16.33.30-300_Port5.0	VLANIF Port Problem at Port=5.0 on 172.16.33.30	Aug 03,2004 02:48:13 PM
Major	VLANIF-172.16.33.30-301_Port5.0	VLANIF Port Problem at Port=5.0 on 172.16.33.30	Aug 03,2004 02:48:13 PM
Major	Ether-like_172.16.33.30_Port5.0	Link Down on Port=5.0 -- SNMP Trap Vars: sysUpTime=3 hours, 28...	Aug 03,2004 02:48:13 PM
Minor	PD_PD-172.16.33.30-nms_stateChange	EPSR Domain State-Change from LINKS-UP to LINK-DOWN - SN...	Aug 03,2004 02:48:13 PM
Minor	172.16.33.20	Node failure. This probably means one or more interfaces have fai...	Aug 03,2004 02:48:12 PM
Major	VLANIF-172.16.33.20-501_Port11.1	VLANIF Port Problem at Port=11.1 on 172.16.33.20	Aug 03,2004 02:48:12 PM
Major	VLANIF-172.16.33.20-700_Port11.1	VLANIF Port Problem at Port=11.1 on 172.16.33.20	Aug 03,2004 02:48:12 PM
Major	VLANIF-172.16.33.20-1_Port11.1	VLANIF Port Problem at Port=11.1 on 172.16.33.20	Aug 03,2004 02:48:12 PM
Major	VLANIF-172.16.33.20-300_Port11.1	VLANIF Port Problem at Port=11.1 on 172.16.33.20	Aug 03,2004 02:48:12 PM
Major	VLANIF-172.16.33.20-301_Port11.1	VLANIF Port Problem at Port=11.1 on 172.16.33.20	Aug 03,2004 02:48:12 PM
Major	LINK-172.16.33.30-5.0--172.16.33.20-11.1_Node172.1...	Link Port Problem at Port=11.1 on 172.16.33.20	Aug 03,2004 02:48:12 PM
Major	Ether-like_172.16.33.20_Port11.1	Link Down on Port=11.1 -- SNMP Trap Vars: sysUpTime=3 hours, 1...	Aug 03,2004 02:48:12 PM
Minor	PD_PD-172.16.33.20-nms_stateChange	EPSR Domain State-Change from LINKS-UP to LINK-DOWN - SN...	Aug 03,2004 02:48:12 PM
Minor	PD_PD-172.16.68.80-nms_stateChange	EPSR Domain State-Change from COMPLETE to FAILED - SNMP v...	Aug 03,2004 02:48:11 PM

FIGURE 16-80 Alarms of EPSR with FAILED state

16.10.6.3 EPSR Failed (No Ports for Data Flow on Device(s)

When both paths are broken there is no data path to or from a device, so data service is lost on that port. In this case, the map GUI and alarms reflect this loss of service situation.

- Protection Ring - Both links for device .20 are shown as blocked, so data traffic for this Protection VLAN cannot be received or transmitted on the device.

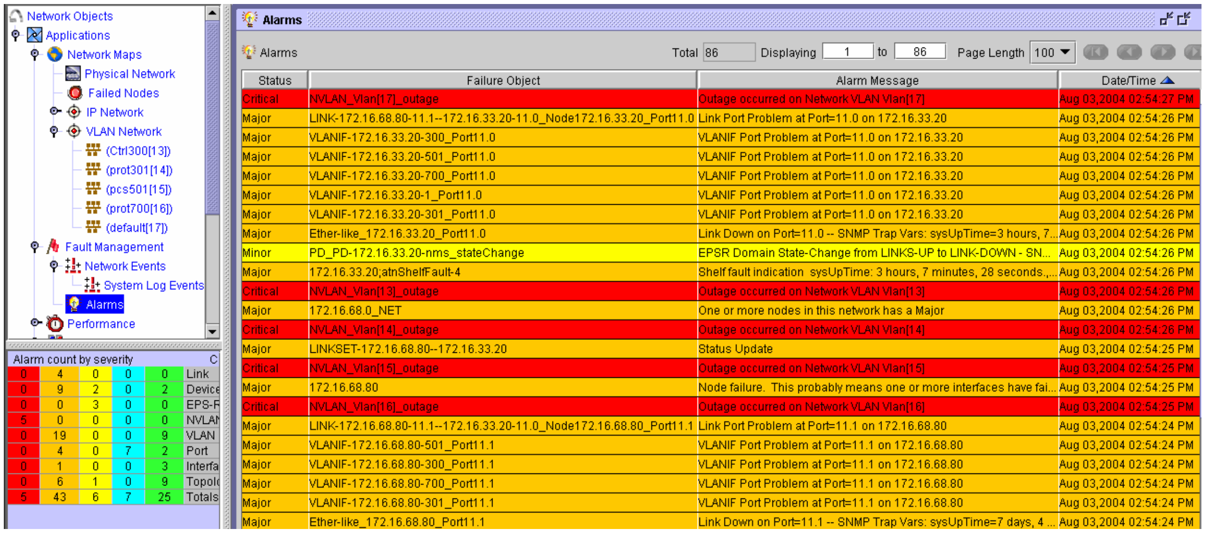


Alarm count by severity

					C
0	4	0	0	0	Link
0	9	2	0	2	Device
0	0	3	0	0	EPS-R
5	0	0	0	0	NVLAN

FIGURE 16-81 Protection VLAN prot300 when Both Ports Down

- Alarms - Viewing the alarms shows all of the associated alarms, as highlighted below.



Alarm count by severity C

0	4	0	0	0	Link
0	9	2	0	2	Device
0	0	3	0	0	EPS-R
5	0	0	0	0	NVLAN
0	19	0	0	9	VLAN
0	4	0	7	2	Port
0	1	0	0	3	Interfa
0	6	1	0	9	Topolo
5	43	6	7	25	Totals

Total 86 Displaying 1 to 86 Page Length 100

Status	Failure Object	Alarm Message	Date/Time
Critical	NVLAN_Vlan[17]_outage	Outage occurred on Network VLAN Vlan[17]	Aug 03,2004 02:54:27 PM
Major	LINK-172.16.68.80-11.1--172.16.33.20-11.0_Node172.16.33.20_Port11.0	Link Port Problem at Port=11.0 on 172.16.33.20	Aug 03,2004 02:54:26 PM
Major	VLANIF-172.16.33.20-300_Port11.0	VLANIF Port Problem at Port=11.0 on 172.16.33.20	Aug 03,2004 02:54:26 PM
Major	VLANIF-172.16.33.20-501_Port11.0	VLANIF Port Problem at Port=11.0 on 172.16.33.20	Aug 03,2004 02:54:26 PM
Major	VLANIF-172.16.33.20-700_Port11.0	VLANIF Port Problem at Port=11.0 on 172.16.33.20	Aug 03,2004 02:54:26 PM
Major	VLANIF-172.16.33.20-1_Port11.0	VLANIF Port Problem at Port=11.0 on 172.16.33.20	Aug 03,2004 02:54:26 PM
Major	VLANIF-172.16.33.20-301_Port11.0	VLANIF Port Problem at Port=11.0 on 172.16.33.20	Aug 03,2004 02:54:26 PM
Major	Ether-like_172.16.33.20_Port11.0	Link Down on Port=11.0 -- SNMP Trap Vars: sysUpTime=3 hours, 7...	Aug 03,2004 02:54:26 PM
Minor	PD_PD-172.16.33.20-nms_stateChange	EPSR Domain State-Change from LINKS-UP to LINK-DOWN - SN...	Aug 03,2004 02:54:26 PM
Major	172.16.33.20;atnShelfFault-4	Shelf fault indication sysUpTime: 3 hours, 7 minutes, 28 seconds.,...	Aug 03,2004 02:54:26 PM
Critical	NVLAN_Vlan[13]_outage	Outage occurred on Network VLAN Vlan[13]	Aug 03,2004 02:54:26 PM
Major	172.16.68.0_NET	One or more nodes in this network has a Major	Aug 03,2004 02:54:26 PM
Critical	NVLAN_Vlan[14]_outage	Outage occurred on Network VLAN Vlan[14]	Aug 03,2004 02:54:26 PM
Major	LINKSET-172.16.68.80--172.16.33.20	Status Update	Aug 03,2004 02:54:25 PM
Critical	NVLAN_Vlan[15]_outage	Outage occurred on Network VLAN Vlan[15]	Aug 03,2004 02:54:25 PM
Major	172.16.68.80	Node failure. This probably means one or more interfaces have fai...	Aug 03,2004 02:54:25 PM
Critical	NVLAN_Vlan[16]_outage	Outage occurred on Network VLAN Vlan[16]	Aug 03,2004 02:54:25 PM
Major	LINK-172.16.68.80-11.1--172.16.33.20-11.0_Node172.16.68.80_Port11.1	Link Port Problem at Port=11.1 on 172.16.68.80	Aug 03,2004 02:54:24 PM
Major	VLANIF-172.16.68.80-501_Port11.1	VLANIF Port Problem at Port=11.1 on 172.16.68.80	Aug 03,2004 02:54:24 PM
Major	VLANIF-172.16.68.80-300_Port11.1	VLANIF Port Problem at Port=11.1 on 172.16.68.80	Aug 03,2004 02:54:24 PM
Major	VLANIF-172.16.68.80-700_Port11.1	VLANIF Port Problem at Port=11.1 on 172.16.68.80	Aug 03,2004 02:54:24 PM
Major	VLANIF-172.16.68.80-301_Port11.1	VLANIF Port Problem at Port=11.1 on 172.16.68.80	Aug 03,2004 02:54:24 PM
Major	Ether-like_172.16.68.80_Port11.1	Link Down on Port=11.1 -- SNMP Trap Vars: sysUpTime=7 days, 4 ...	Aug 03,2004 02:54:24 PM

FIGURE 16-82 Alarm View for EPSR Failure

16.10.7 Status of Transit Nodes for AlliedWare Plus Devices

When AlliedWare Plus devices, which include the SB x908, x900-12X and -24X series, are included in the EPSR ring as Transit Nodes, their state may or may not reflect any changes that may have occurred. This occurs because the devices fail to send a trap when the EPSR state changes. As a result, only a rediscovery of the nodes can guarantee that the state reflected in the GUIs (such as when selecting *Network Inventory -> EPSR Domains*) is correct.

16.11 SuperLoop Prevention (Superring)

16.11.1 Overview

Prior to release 9.0., if **all** the following conditions were present, a loop could occur between nodes when the EPSR feature was working correctly:

- The network had two or more EPSR domains.
- The protected (data) VLAN overlapped two or more EPSR domains.
- The EPSR domains and the overlapping protected VLANs shared a common link.

When there was a common link failure, each ring would block the appropriate interface, but this could lead to a larger loop, or SuperLoop, being created. Because of this, EPSR rings that had all the attributes listed above were not allowed.

To resolve the SuperLoop issue, the concept of certain ring interfaces having a priority is introduced. This priority is assigned to the control VLAN on the interface. The value range is 0 to 127. By default, the priority of each of the ring interfaces for an EPSR domain is 0 (the lowest priority), and means there is no change in how the interface and protocol works prior to release 9.0. The higher values, however, are used when there are interconnected EPSR rings in which the SuperLoop condition needs to be avoided.

When creating this configuration, which is called a SuperRing, the user will therefore specify an EPSR Priority when an EPS Ring is created. When the user enters a value greater than 0, this indicates the ring is intended to be used with other peer rings to form a SuperRing. If the user sets the priority to 0, then the ring will behave as an ordinary EPS Ring as described in "Protection Switching-EPSR" on page 567.

As with creating regular EPS Rings, the user should first decide on the VLANs and topologies to be used based on iMAP recommendations.

The following figure shows how the feature would work with two EPSR rings and an interconnected data VLAN over a common physical link. This configuration will be the result of using the AlliedView NMS SuperLoop feature that makes up the rest of this Section.

Note that there are several configuration rules that must be followed since there can be multiple ring domains that share one or more protected VLANs. These rules are described in detail in the *Software Reference for iMAP Series Switches*. By using the AlliedView NMS to create an EPSR SuperLoop configuration and following a recommended series of steps, the user can ensure that these rules are automatically followed. Moreover, there are appropriate warning messages when the user should be made aware of changes that are being made to a configuration.

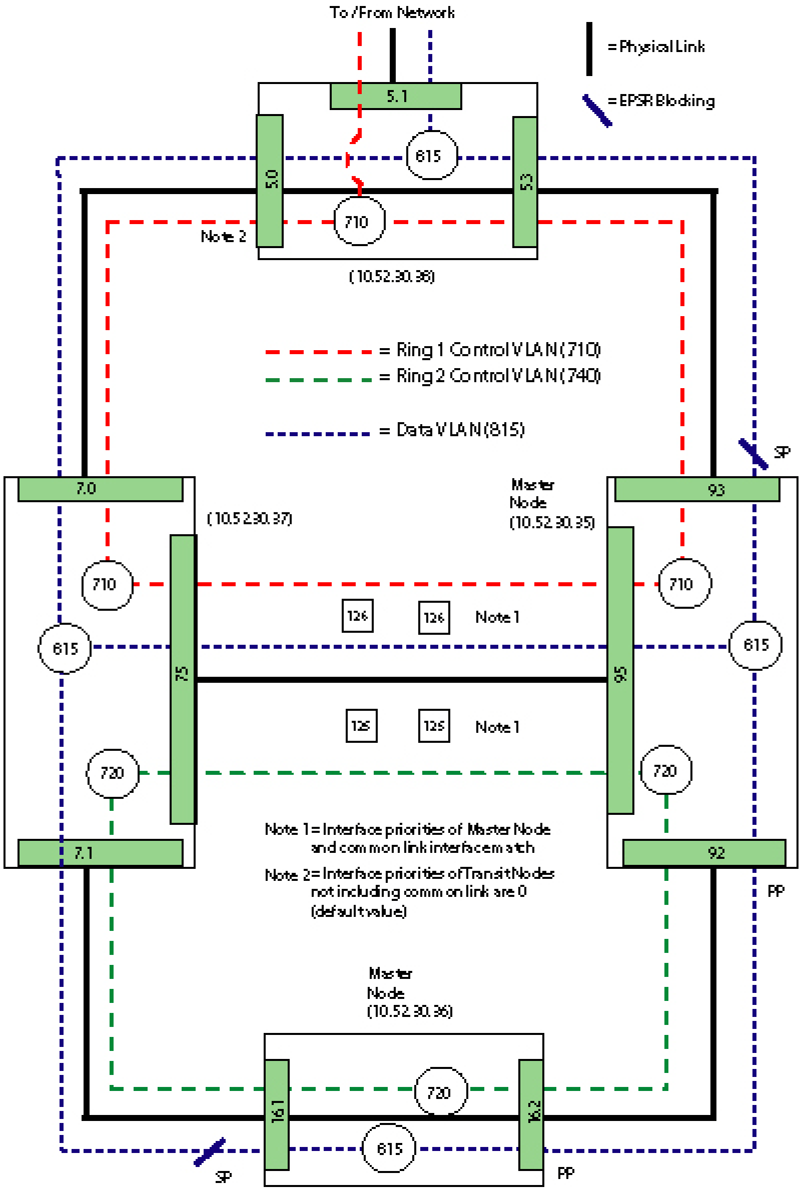

To /From Network
=Physical Link
=EPSR Blocking
5.1
5.0
5.3
615
710
Note 2
(10.52.30.38)
= Ring 1 Control VLAN (710)
= Ring 2 Control VLAN (740)
= Data VLAN (815)
SP
7.0
93
(10.52.30.37)
Master Node (10.52.30.35)
710
710
126
126
Note 1
615
615
75
95
125
125
Note 1
720
720
7.1
92
Note 1 = Interface priorities of Master Node and common link interface match
Note 2 = Interface priorities of Transit Nodes not including common link are 0 (default value)
PP
Master Node (10.52.30.36)
16.1
16.2
720
615
SP
PP

FIGURE 16-83 Example Configuration for SuperLoop Feature

Following the example shown in the figure, the user wishes to have one ring at priority 126 and the other at 125. The major steps to create this configuration are as follows:

1. Create the first EPS Ring with a Control VLAN of 710, with a domain name of ctrl710. This is the same as creating an EPS Ring is Section "Protection Switching-EPSR" on page 567, but the user specifies Priority=126.
2. Create a second EPS Ring with the Control VLAN for 720 and the domain name ctrl720. For this ring, specify Priority=125. Since the rings are to be peers, the iMAPs that contain the shared ports will not permit the domains to be enabled at this point. (not until they have at least one common data VLAN).
3. If the SuperRing is to have more rings on it, add them one-by-one as they connect to the existing rings.
4. To add a protected data VLAN to the SuperRing, select **any** one of the Peer control VLAN maps and create a protected VLAN. **This VLAN will automatically be extended to the entire SuperRing domain** (all of the EPSR domains that make up the SuperRing).
5. Any EPSR domains that are disabled can now be enabled.

At the end of the procedure, all created rings are part of the SuperRing, and any Protected VLANs created on the original ring will be protected by the SuperRing domain.

Additional Protected VLANs can be added after the Super-Ring is created by selecting any one of the control ring maps and creating a protected VLAN on it. The NMS will automatically extend that data VLAN to all of the peer domains. This permits creation of protected VLANs without disabling the Super-Ring, since the iMAP requires the protection to be configured on all peer domains of a device at the same time.

16.11.2 Creating the EPSR SuperRIng

16.11.2.1 Create a Network VLAN and with it Create an EPSR Control VLAN

These steps are similar to those described in "Creating Network VLANs" on page 533 and "Protection Switching-EPSR" on page 567. The user selects one or more nodes on the Physical Network map and by using the Create VLAN Net Form creates a loop VLAN that includes the appropriate nodes and interfaces. The user then turns this Network VLAN into an EPSR Control VLAN (creating the EPSR domain) by right clicking on the GUI of the Network VLAN that is a ring and selecting “Configure EPS Control Ring”.

Note: *The user can also choose the VLAN Operations menu pull-down.*

Making this choice brings up the Configure EPS Control Ring Panel, as shown in the following figures.

Note: *When a network VLAN has been configured as a ring, the icon for a ring appears as the leaf in the VLAN Network tree hierarchy.*

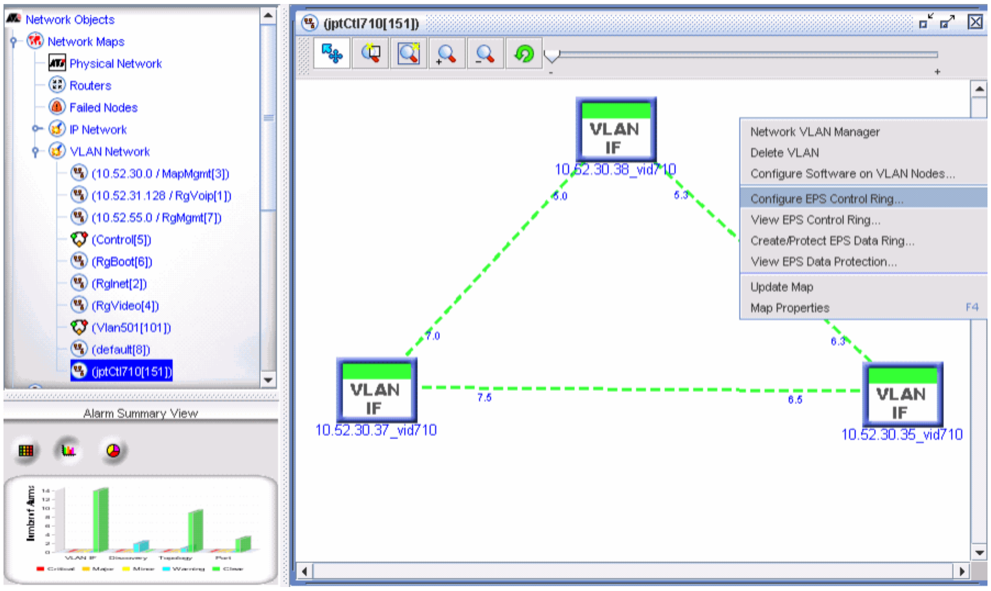


FIGURE 16-84 Configure EPS Control Ring Menu Item

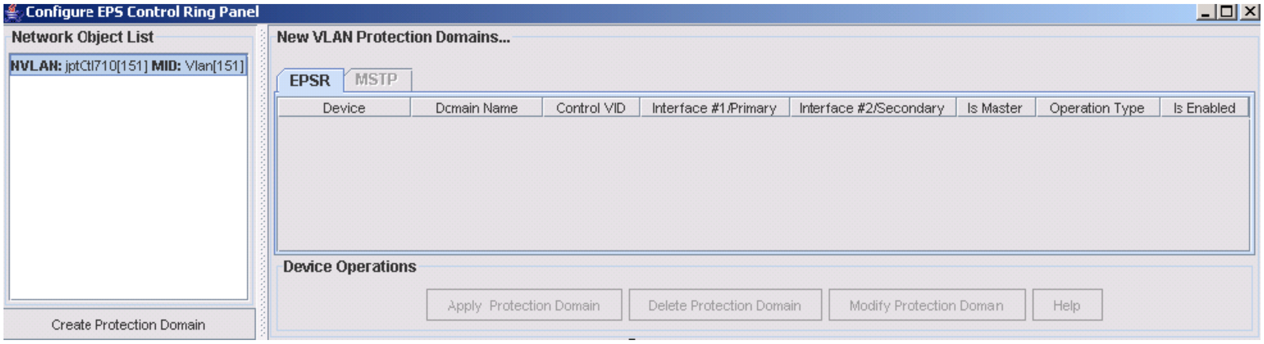
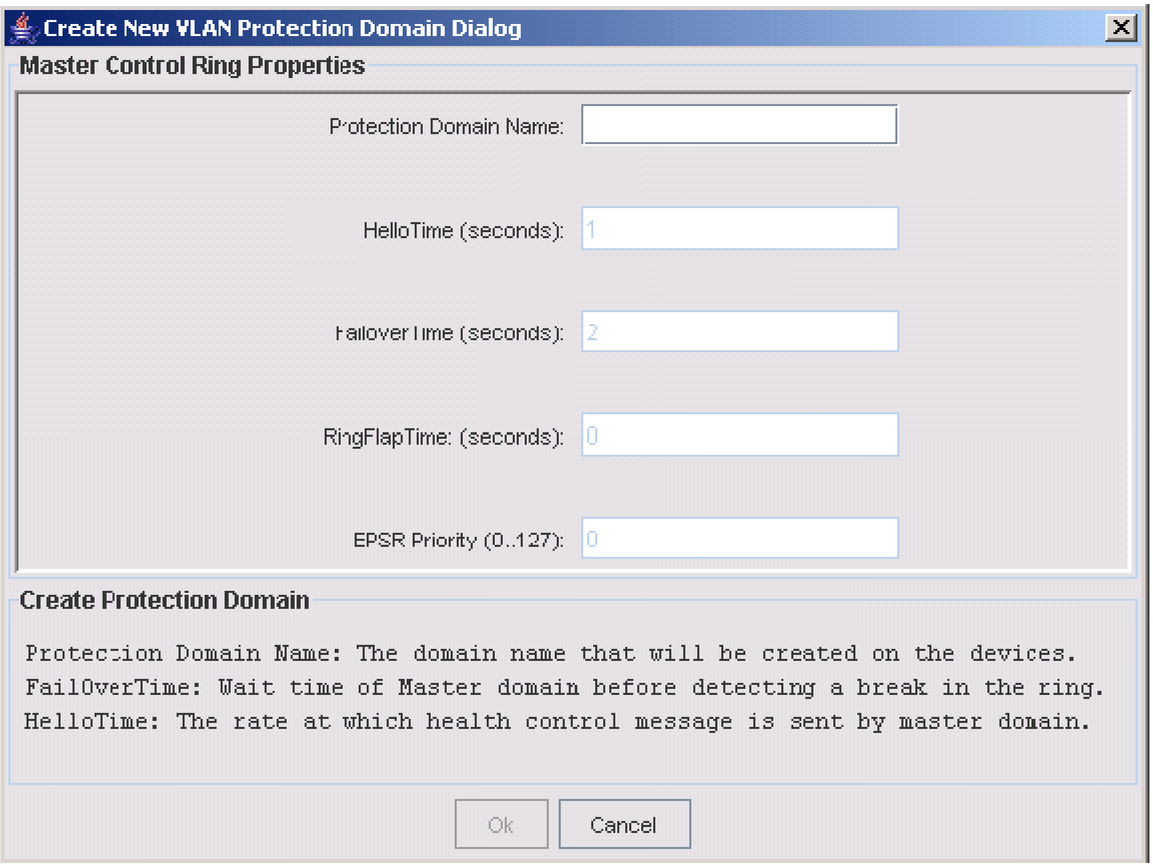


FIGURE 16-85 Configure EPS Control Ring Panel

The Network VLAN should be highlighted on the left panel. (If not select the loop Network VLAN), then select "Create Protection Domain". This brings up the Create New VLAN Protection Domain Dialog Form, as shown in the following figure.


Create New VLAN Protection Domain Dialog
Master Control Ring Properties
Create Protection Domain
Ok
Cancel

Protection Domain Name:

HelloTime (seconds): 1

FailoverTime (seconds): 2

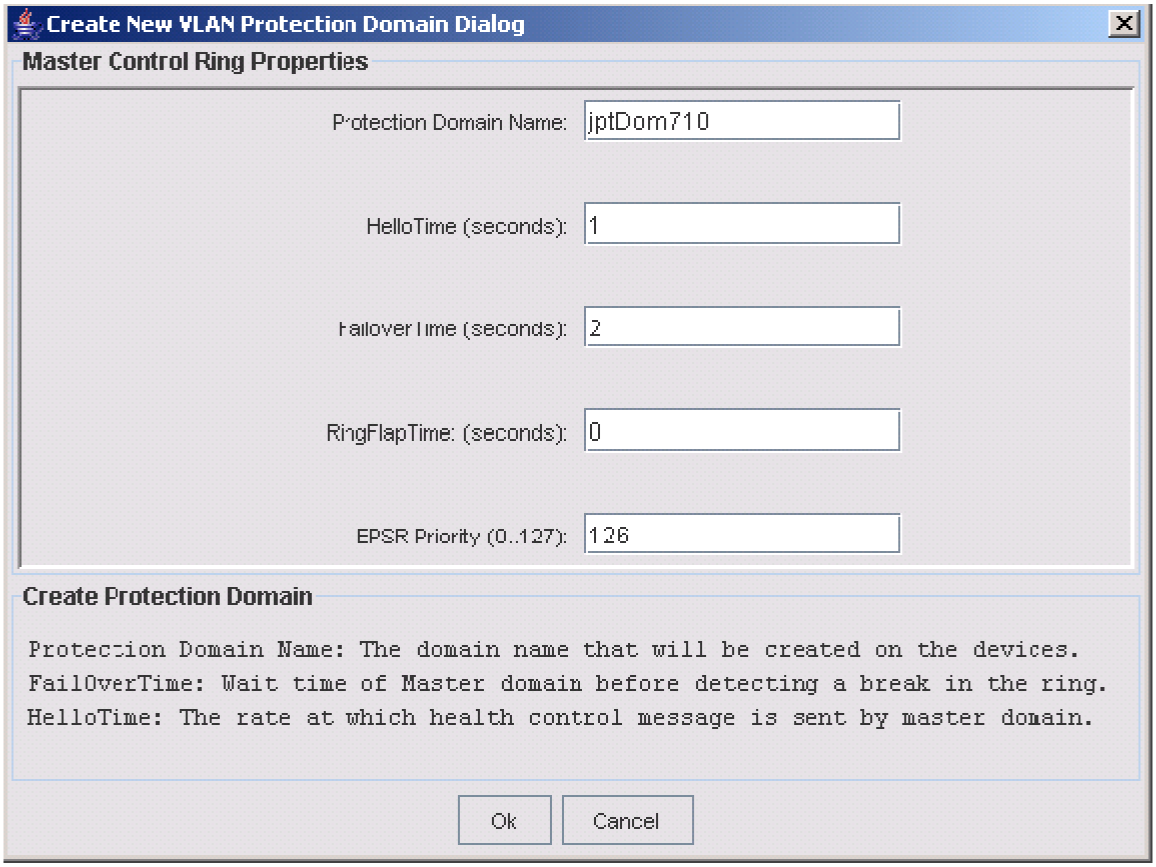
RingFlapTime: (seconds): 0

EPSR Priority (0..127): 0

Protection Domain Name: The domain name that will be created on the devices.
FailOverTime: Wait time of Master domain before detecting a break in the ring.
HelloTime: The rate at which health control message is sent by master domain.

FIGURE 16-86 Create New VLAN Protection Domain Dialog (Initial)

Enter the **Protection Domain Name** = jptDom710 and the **EPSR Priority**=126. By putting in a non-zero value, the user intends to use the this EPS Ring in a SuperRing configuration. Finish by selecting OK, and the system will show how the devices will be configured. Refer to the following figures.



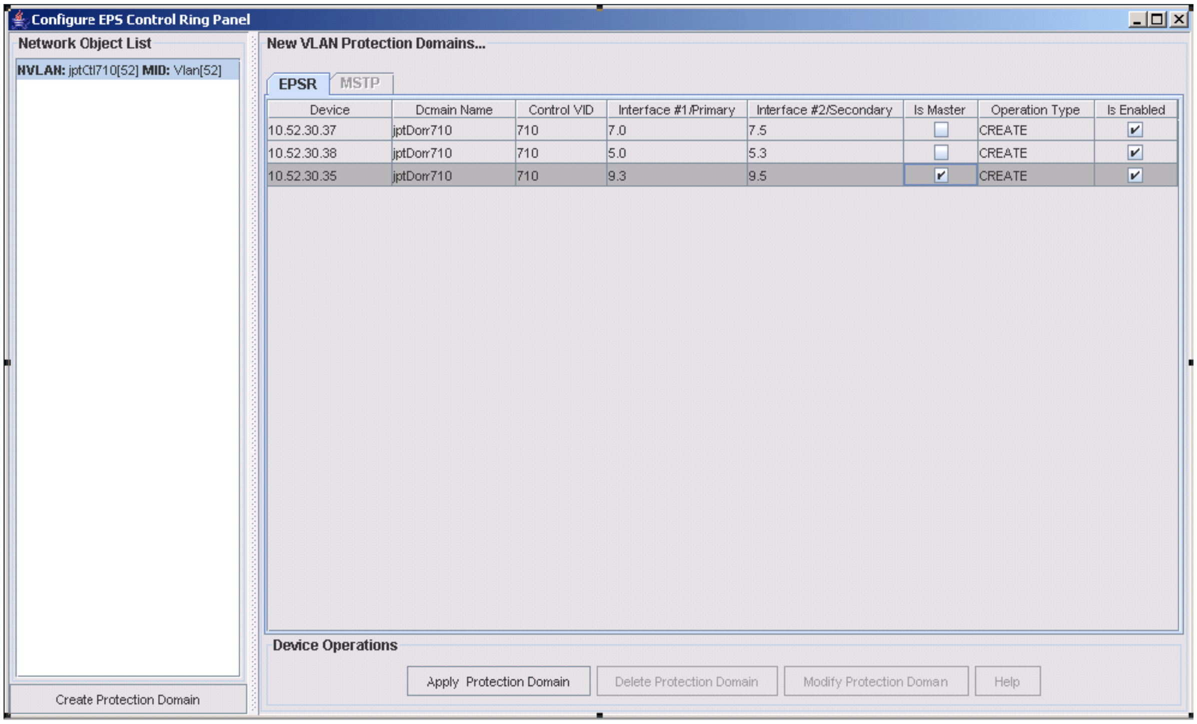
Master Control Ring Properties

Protection Domain Name:	jptDom710
HelloTime (seconds):	1
Failover Time (seconds):	2
RingFlapTime: (seconds):	0
EPSR Priority (0..127):	126

Create Protection Domain

```
Protection Domain Name: The domain name that will be created on the devices.
FailOverTime: Wait time of Master domain before detecting a break in the ring.
HelloTime: The rate at which health control message is sent by master domain.
```

FIGURE 16-87 Create New VLAN Protection Domain Dialog (Complete)



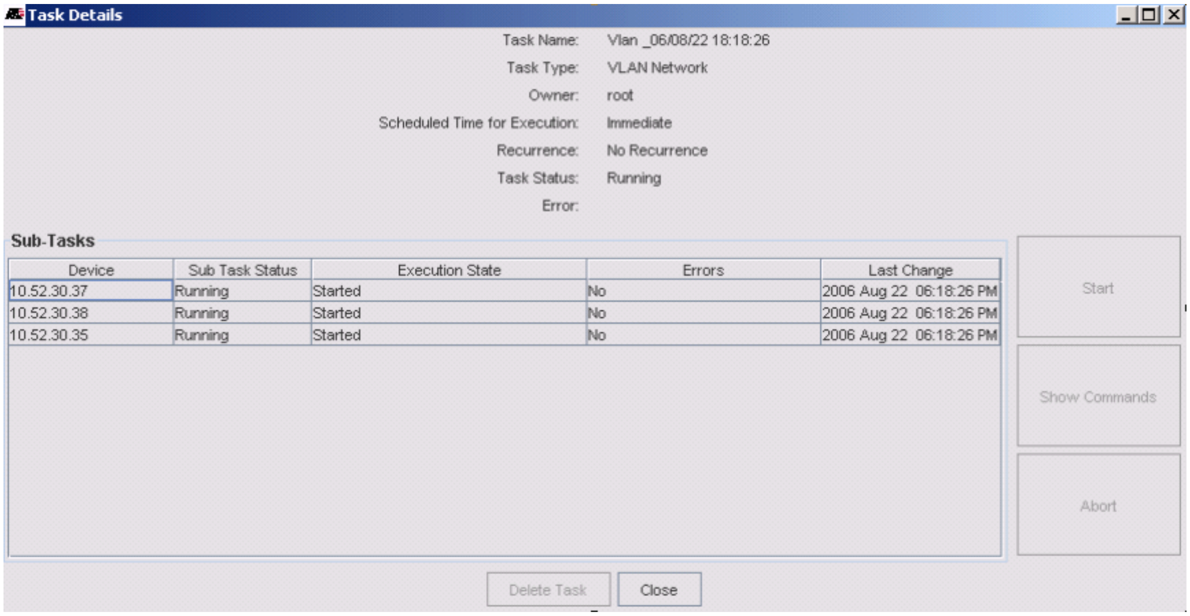
NVLAN: jptCtl710[52] **MID:** Vlan[52]

New VLAN Protection Domains...

Device	Dcmain Name	Control VID	Interface #1/Primary	Interface #2/Secondary	Is Master	Operation Type	Is Enabled
10.52.30.37	jptDom710	710	7.0	7.5	□	CREATE	☑
10.52.30.38	jptDom710	710	5.0	5.3	□	CREATE	☑
10.52.30.35	jptDom710	710	9.3	9.5	☑	CREATE	☑

FIGURE 16-88 Create New VLAN Protection Domain (Task List)

The figure above shows the components of the EPSR Domain that are to be created at each node. After the Domain is created, then the VLAN interfaces of the selected loop NVLAN (top left) will be added to the Domain as control VLANs. Click on the “Apply Protection Domain” button to activate the tasks. AlliedView NMS will execute these tasks on each device (called Sub-Tasks) in parallel, and provide progress messages for each Sub-Task, as shown in the following figure.



Task Details

Task Name: Vlan _06/08/22 18:18:26
Task Type: VLAN Network
Owner: root
Scheduled Time for Execution: Immediate
Recurrence: No Recurrence
Task Status: Running
Error:

Sub-Tasks

Device	Sub Task Status	Execution State	Errors	Last Change
10.52.30.37	Running	Started	No	2006 Aug 22 06:18:26 PM
10.52.30.38	Running	Started	No	2006 Aug 22 06:18:26 PM
10.52.30.35	Running	Started	No	2006 Aug 22 06:18:26 PM

FIGURE 16-89 Task Progress for Creating EPS Ring (part of SuperRing)

When finished, an EPS Ring is created in which all the associated devices have the control VLAN configured on the relevant interface, and one node designated as the Master, as shown in the following figure.

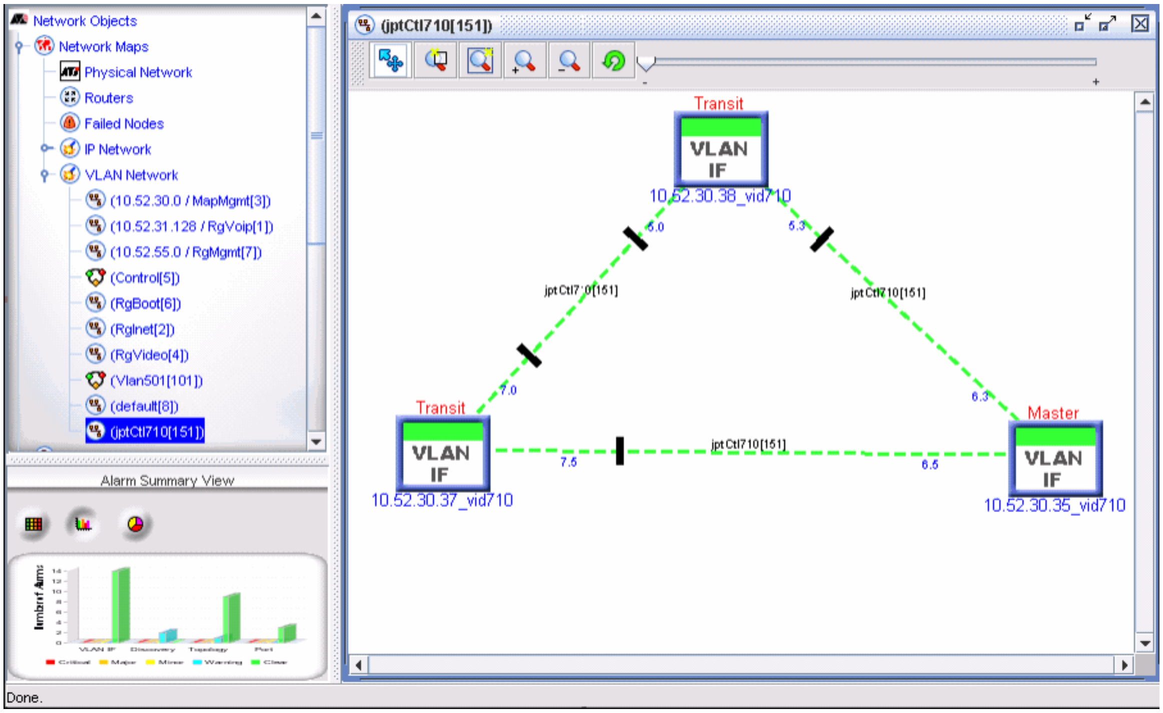


FIGURE 16-90 EPS Ring Created (First Ring of SuperRing)

16.11.2.2 Create Second EPS Ring that is a Peer of First EPS Ring

The steps to create the second, peer EPS Ring are similar to the first. In choosing a looped Network VLAN where there is a shared link with another EPS Ring, the user must put in a non-zero value for the EPSR Priority, and this value must be different than the first ring.

Select the Network VLAN and click on Create Protection Domain. As with the first EPS Ring, the Control VLAN is configured on all of the interfaces and the resulting GUI shows the EPS Ring and which node is Master, as shown in the following figures.

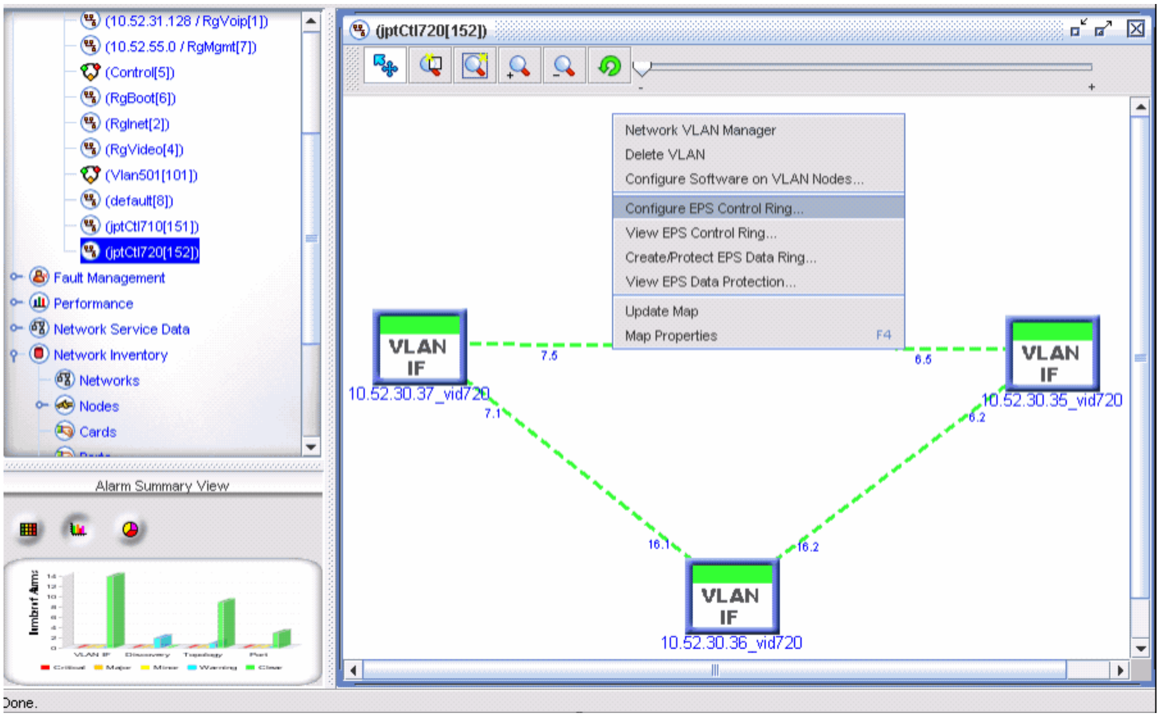
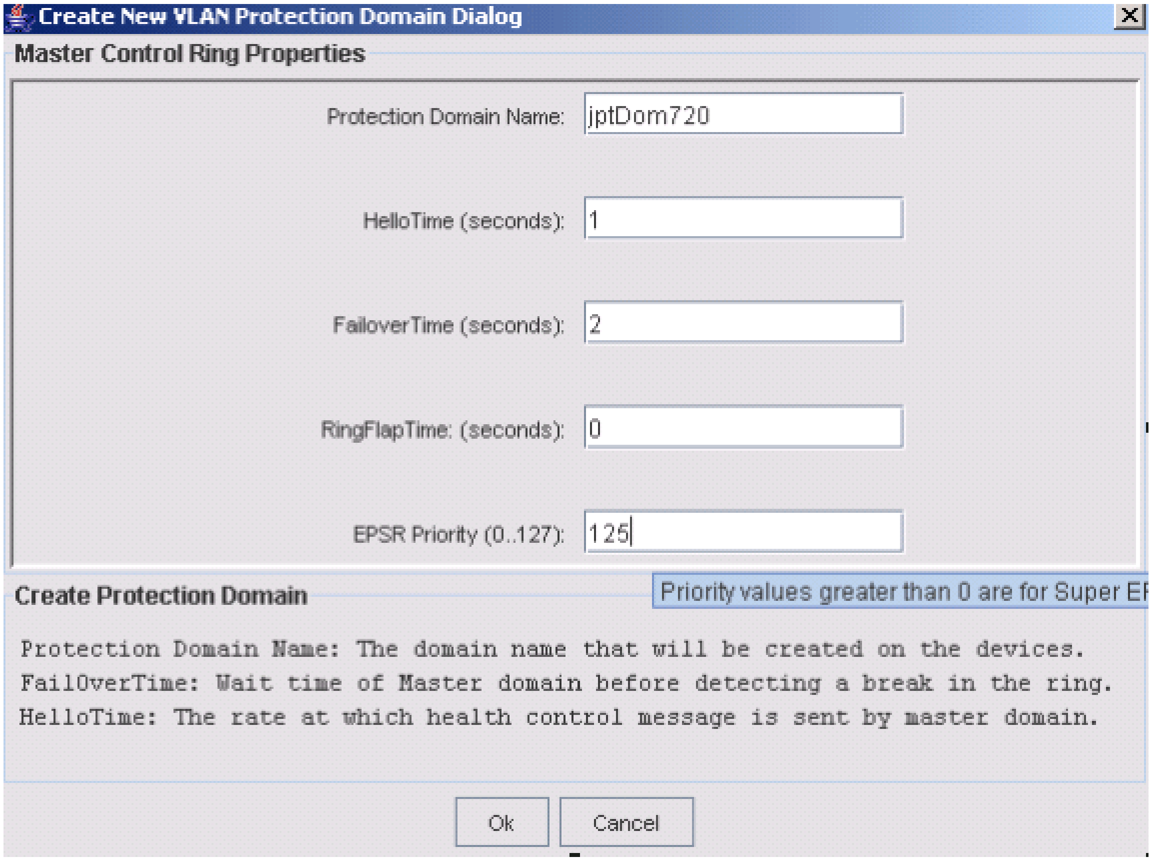


FIGURE 16-91 Configure Peer EPS Ring (to form SuperRing Configuration)


Create New VLAN Protection Domain Dialog
Master Control Ring Properties

Protection Domain Name: jptDom720

HelloTime (seconds): 1

FailoverTime (seconds): 2

RingFlapTime: (seconds): 0

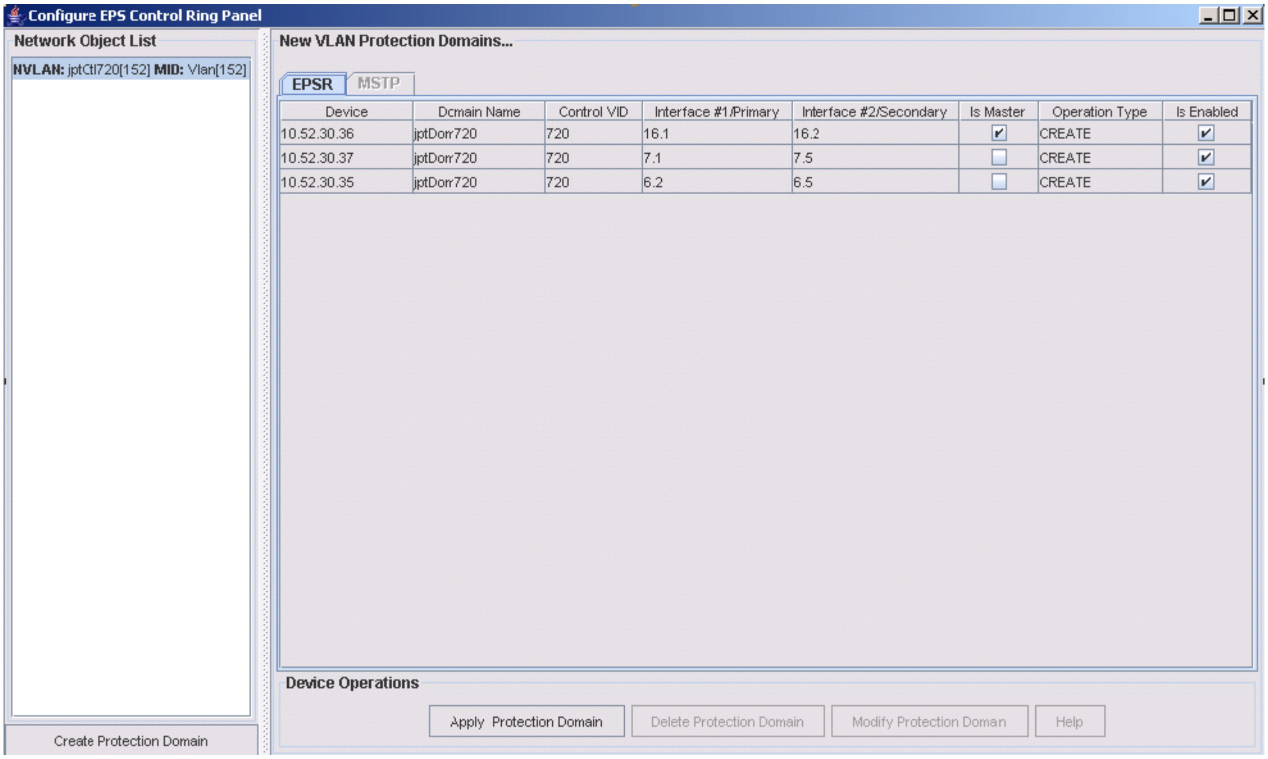
EPSR Priority (0..127): 125

Priority values greater than 0 are for Super EI

```
Protection Domain Name: The domain name that will be created on the devices.
FailOverTime: Wait time of Master domain before detecting a break in the ring.
HelloTime: The rate at which health control message is sent by master domain.
```

FIGURE 16-92 Configuring the Second EPS Ring with Different EPSR Priority

Finish by selecting OK, and the system will show how the devices will be configured. The user can change the node which will be Master at this point. Refer to the following figure.



NVLAN: jptCtl720[152] **MID:** Vlan[152]

Device	Domain Name	Control VID	Interface #1/Primary	Interface #2/Secondary	Is Master	Operation Type	Is Enabled
10.52.30.36	jptDom720	720	16.1	16.2	☑	CREATE	☑
10.52.30.37	jptDom720	720	7.1	7.5	☐	CREATE	☑
10.52.30.35	jptDom720	720	6.2	6.5	☐	CREATE	☑

FIGURE 16-93 Configure EPS Control Ring Panel for Second Ring

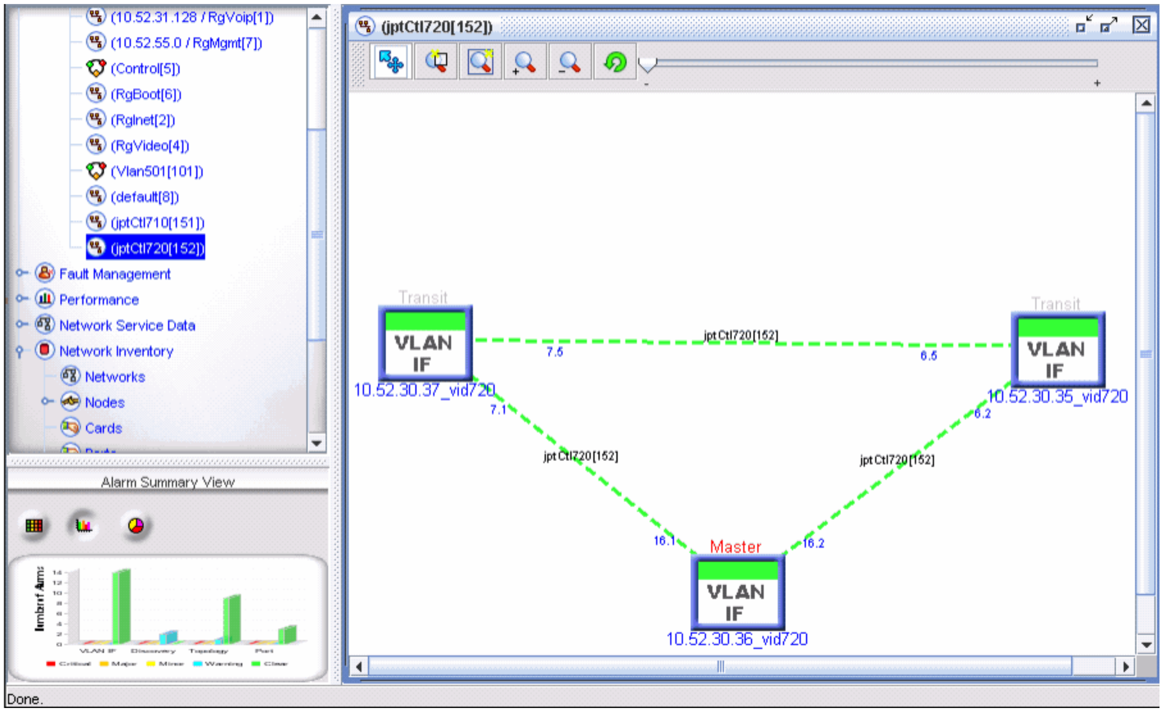


FIGURE 16-94 GUI for Second EPS Ring

The VLAN Link from Port 7.5 on Node 10.52.30.37 to Port 9.5 on Node 10.52.30.35 is now a Shared EPSR Link, since it is also a link of Ring jptCtrl710. **Since the rings jptCtrl720 and jptCtrl710 share a link and both have priorities greater than 0, they are peers forming a Super-Ring**. Also, note that the Transmit Domains are disabled, and they cannot be enabled until the entire SuperRIng has at least one Protected VLAN on it.

16.11.2.3 Creating the Protection VLAN

The “Create/Protect EPS Data Ring…” menu item can now be used from **either** of the Peer maps to create a VLAN that follows the Ring nodes, and is a Protected VLAN of the EPS Ring.

To create the Protected VLAN, right click on one of the Control VLAN maps and select “Create/Protect EPS Data Ring”. The Protect Networked-VLAN Panel appears, as shown in the following figures.

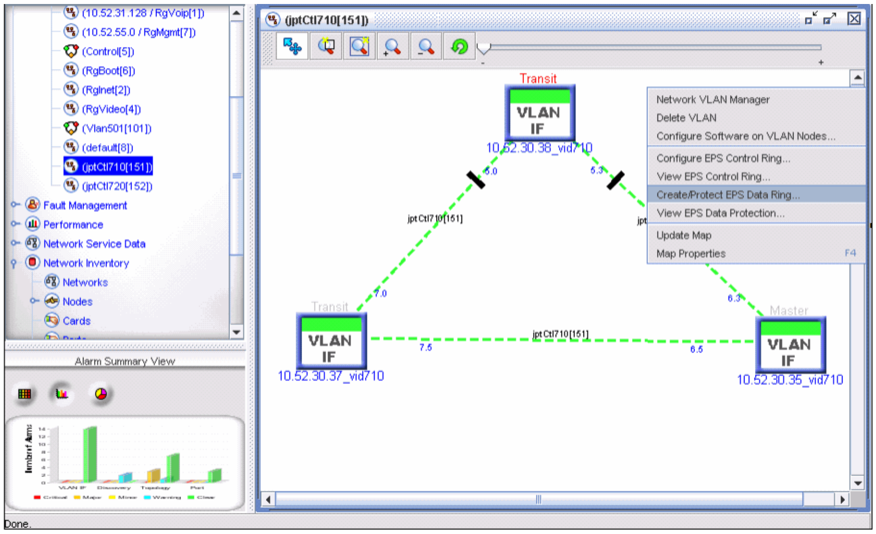


FIGURE 16-95 Selecting Create/Protect EPS Data Ring for the Control VLAN

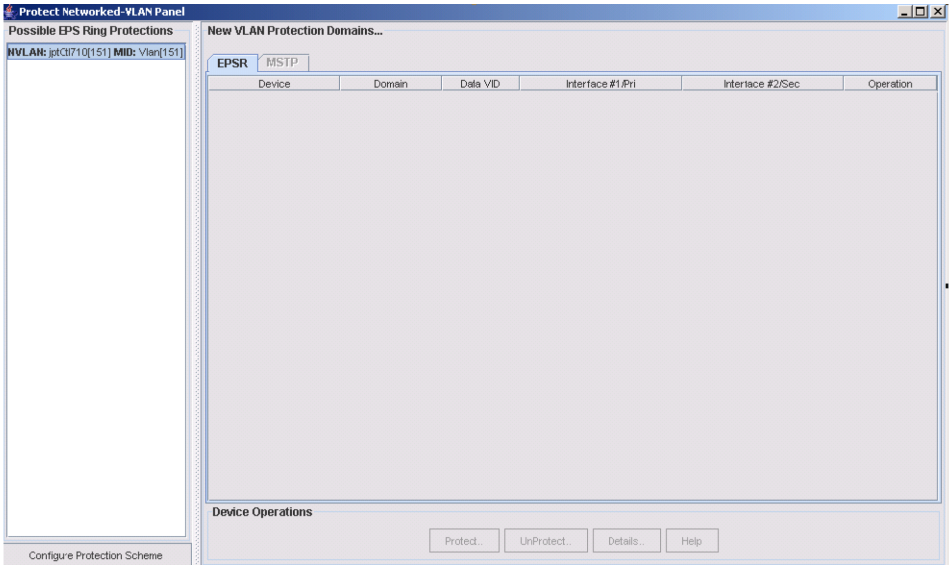
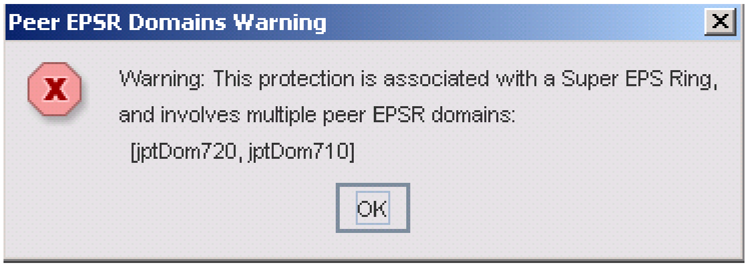

Protect Networked-VLAN Panel
Possible EPS Ring Protections
NVLAN: jptCtl710[151] MID: Vlan[151]
Configure Protection Scheme
New VLAN Protection Domains...
EPSR
MSTP
Device
Domain
Data VID
Interface #1/Pri
Interface #2/Sec
Operation
Device Operations
Protect..
UnProtect..
Details..
Help

FIGURE 16-96 Selecting Network VLAN to Configure as Protection VLAN

After selecting the EPSR Control NVLAN (at the top left) to use as the protecting domain, click on the “Configure Protection Scheme” button.

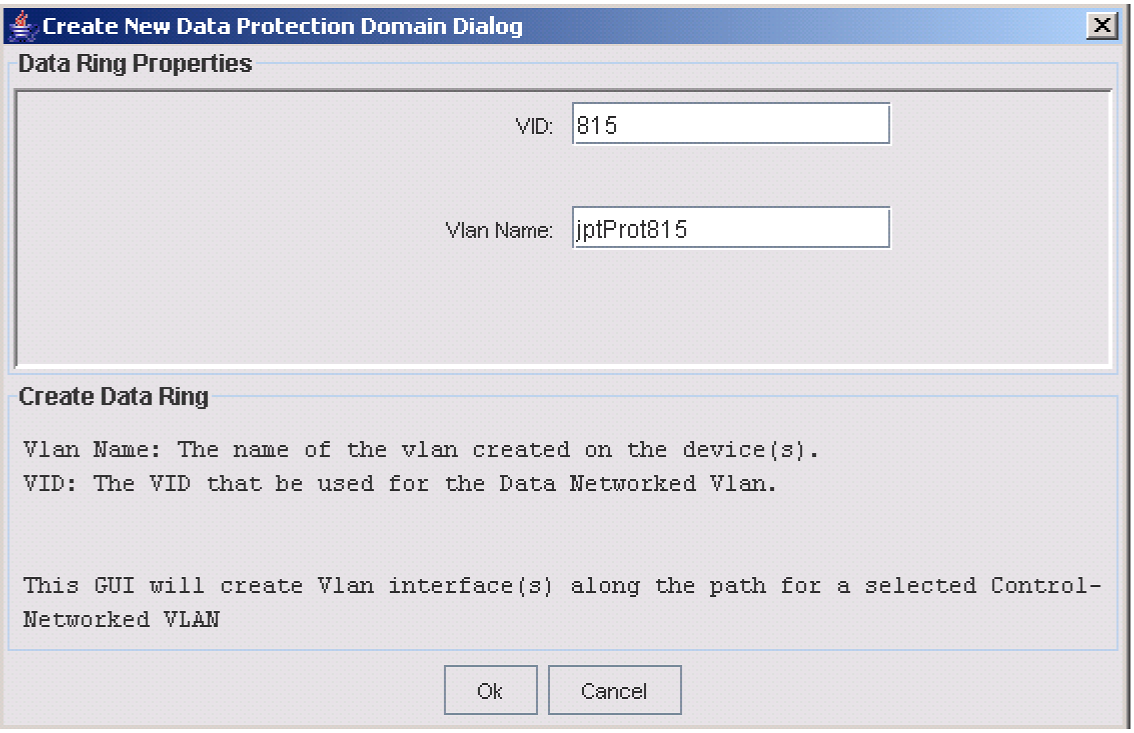
Since the VLAN being created will be protected by multiple peer rings of a Super-Ring, the following warning is displayed:



Warning: This protection is associated with a Super EPS Ring, and involves multiple peer EPSR domains:
[jptDom720, jptDom710]

FIGURE 16-97 Creating Second Protected VLAN for SuperRing - Warning

Fill-in the VID and VLAN Name (for new Protected NVLAN to be created) in the resulting menu



VID: 815

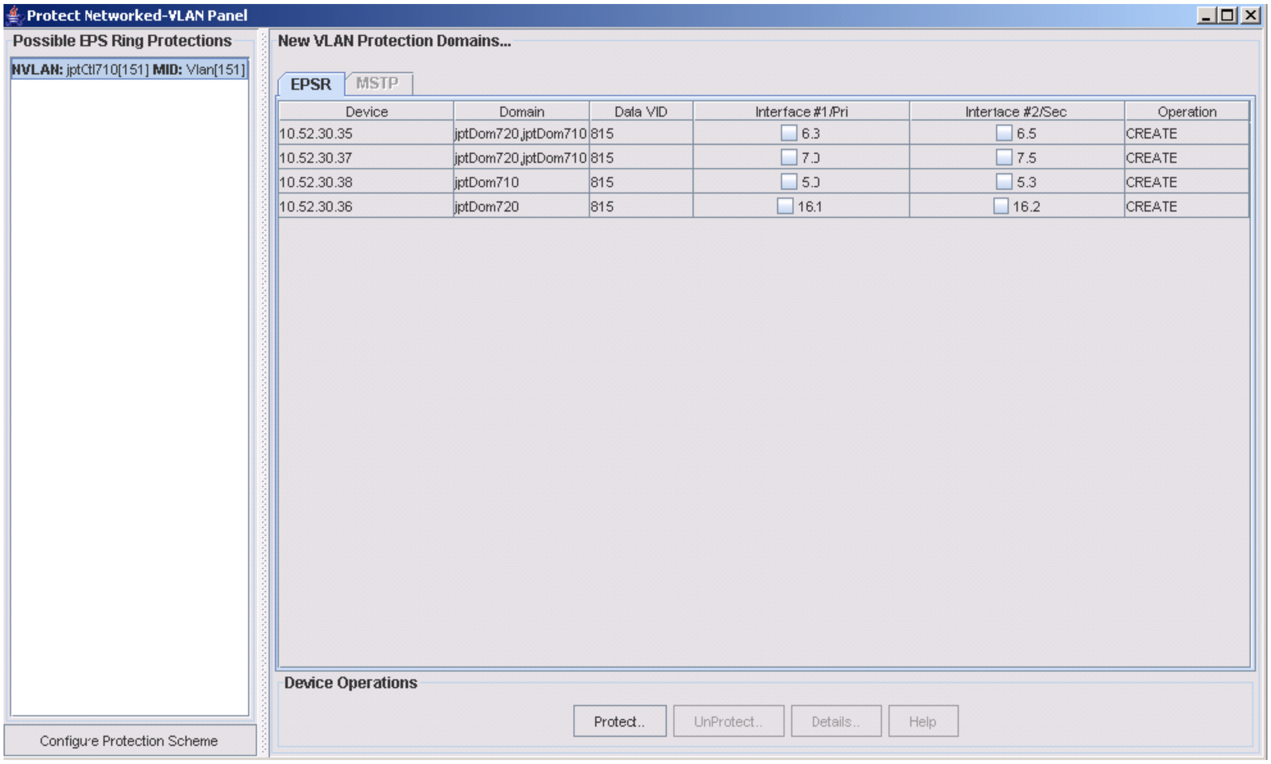
Vlan Name: jptProt815

Vlan Name: The name of the vlan created on the device(s).
VID: The VID that be used for the Data Networked Vlan.

This GUI will create Vlan interface(s) along the path for a selected Control-Networked VLAN

FIGURE 16-98 Configuring the Protected VLAN for Control VLAN

In the above form enter the VLAN ID and the VLAN name. The form notes that this GUI will create the VLAN interfaces along the same path as the Control VLAN. Clicking on OK brings up the Protect Networked-VLAN Panel with the configuration that is going to be created as shown in the following figure.


Protect Networked-VLAN Panel
Possible EPS Ring Protections
New VLAN Protection Domains...
EPSR
MSTP
Device Operations
Protect..
UnProtect..
Details..
Help
Configure Protection Scheme

NVLAN: jptCtl710[151] **MID:** Vlan[151]

Device	Domain	Data VID	Interface #1/Pri	Interface #2/Sec	Operation
10.52.30.35	jptDom720,jptDom710	815	□ 6.3	□ 6.5	CREATE
10.52.30.37	jptDom720,jptDom710	815	□ 7.3	□ 7.5	CREATE
10.52.30.38	jptDom710	815	□ 5.3	□ 5.3	CREATE
10.52.30.36	jptDom720	815	□ 16.1	□ 16.2	CREATE

FIGURE 16-99 Creating the Protection VLAN over multi-EPSR Domains

This table displays the components of the Data VLAN that will cause it to be protected by the Domains indicated in the table. Clicking on the “Protect…” button performs the operations on each device to create the jptProt815 NVLAN and put it into the both Peer Domains, jptDom710 and jptDom720, resulting in the following map for jptProt815.

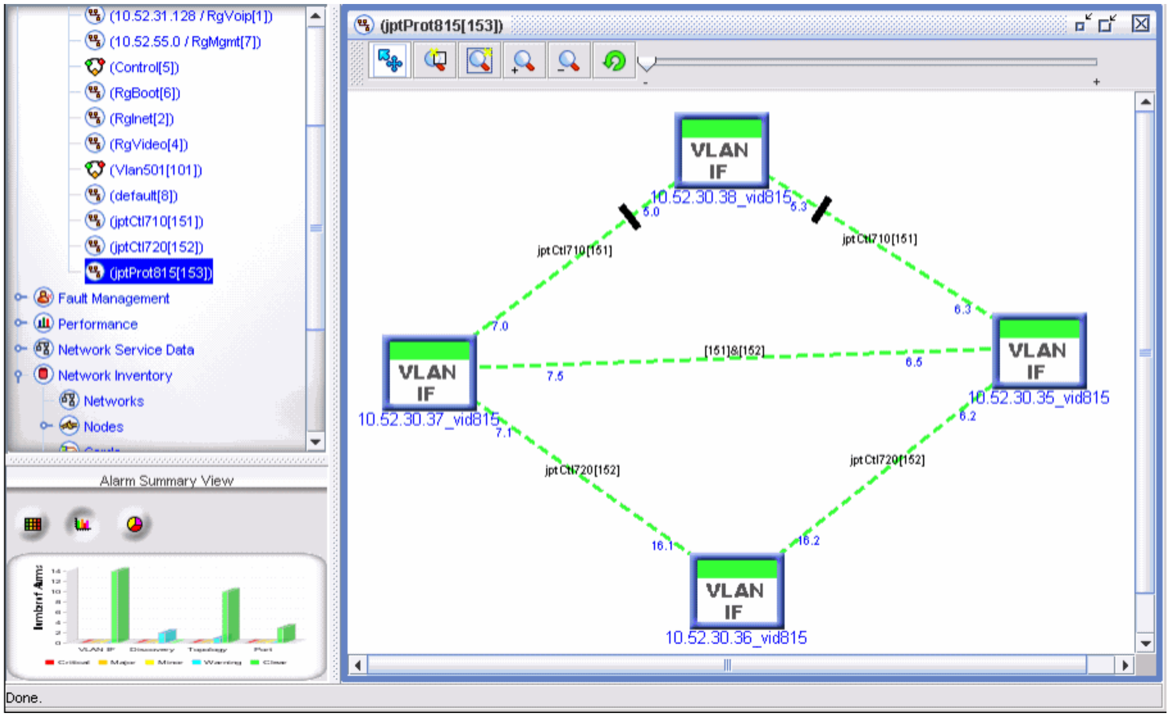


FIGURE 16-100 Superloop Domain

16.11.2.4 Enable the EPS Domains

Now that the SuperRing has at least one Protected VLAN on it, the domains can all be enabled. Select one of the control VLANs and on the map select View EPS Control ring, as shown in the following figure.

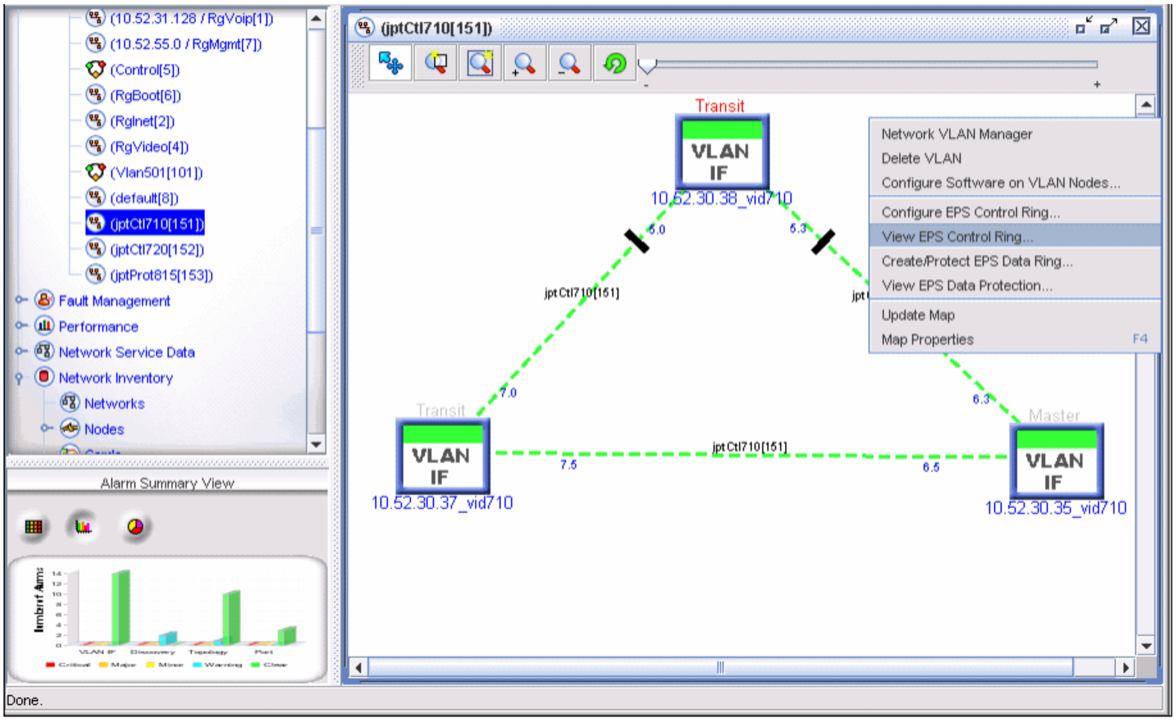
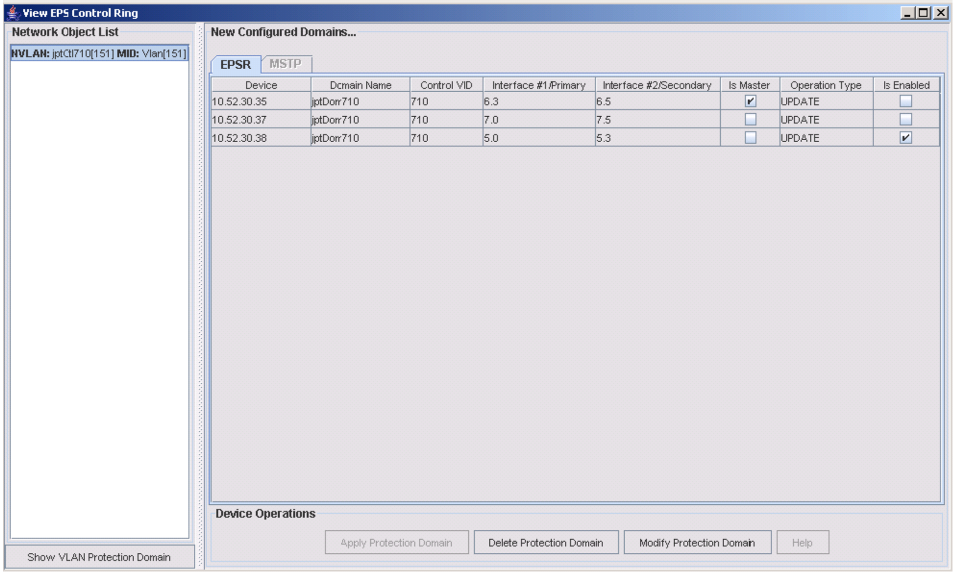


FIGURE 16-101 View one of the EPSR Control Rings


View EPS Control Ring

Network Object List

NVLAN: jptCtl710[151] MID: Vlan[151]

New Configured Domains...

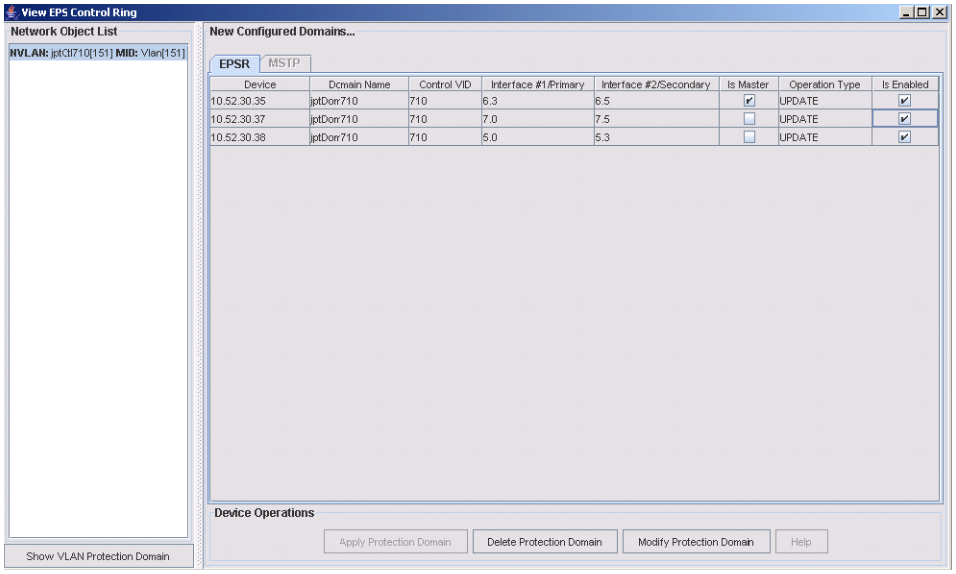
EPSR MSTP

Device	Dcmain Name	Control VID	Interface #1/Primary	Interface #2/Secondary	Is Master	Operation Type	Is Enabled
10.52.30.35	jptDom710	710	6.3	6.5	☑	UPDATE	☐
10.52.30.37	jptDom710	710	7.0	7.5	☐	UPDATE	☐
10.52.30.38	jptDom710	710	5.0	5.3	☐	UPDATE	☑

Device Operations

FIGURE 16-102 View one EPS Control VLAN (used to enable Protection Domain)

Click on the tic boxes under **Is Enabled**, and then **Modify Protection Domain**. When this is done this and the other domains become enabled as well, as shown below.



NVLAN: jptCtl710[151] **MID:** Vlan[151]

Device	Dcmain Name	Control VID	Interface #1/Primary	Interface #2/Secondary	Is Master	Operation Type	Is Enabled
10.52.30.35	jptDom710	710	6.3	6.5	☑	UPDATE	☑
10.52.30.37	jptDom710	710	7.0	7.5	☐	UPDATE	☑
10.52.30.38	jptDom710	710	5.0	5.3	☐	UPDATE	☑

FIGURE 16-103 Protection Domain Enabled

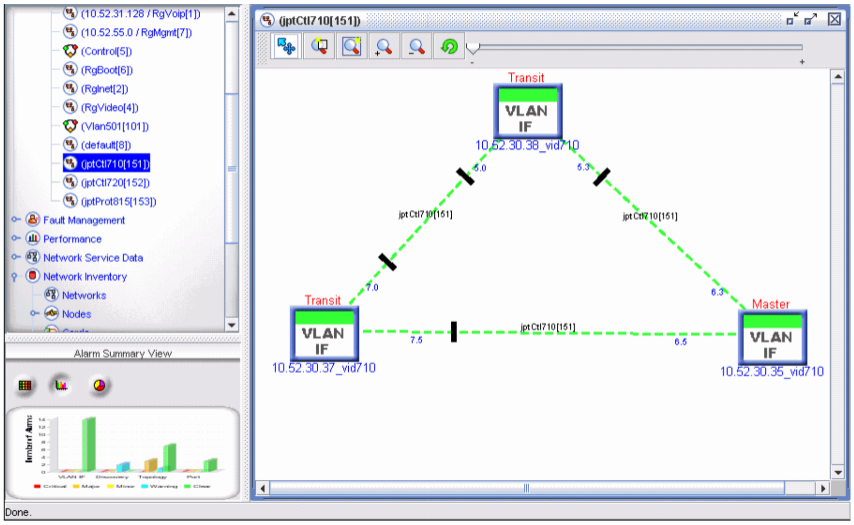


FIGURE 16-104 Enabled Control VLAN (Part of SuperRing)

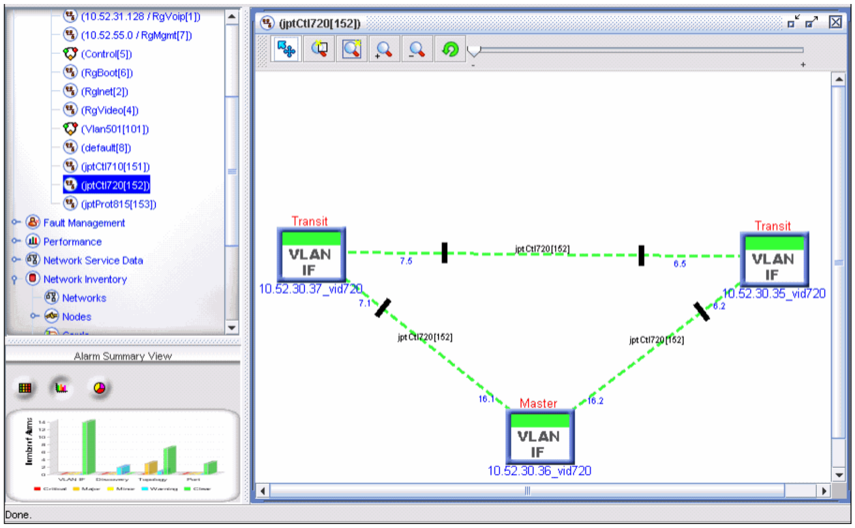


FIGURE 16-105 Enabled Peer Control VLAN (Part of SuperRing)

16.11.2.5 Adding Protected VLANs to the SuperRing

Additional Protected Vlans can be added to Super-Ring by selecting any one of the EPS Rings that make up the SuperRing, as shown in the following figure.

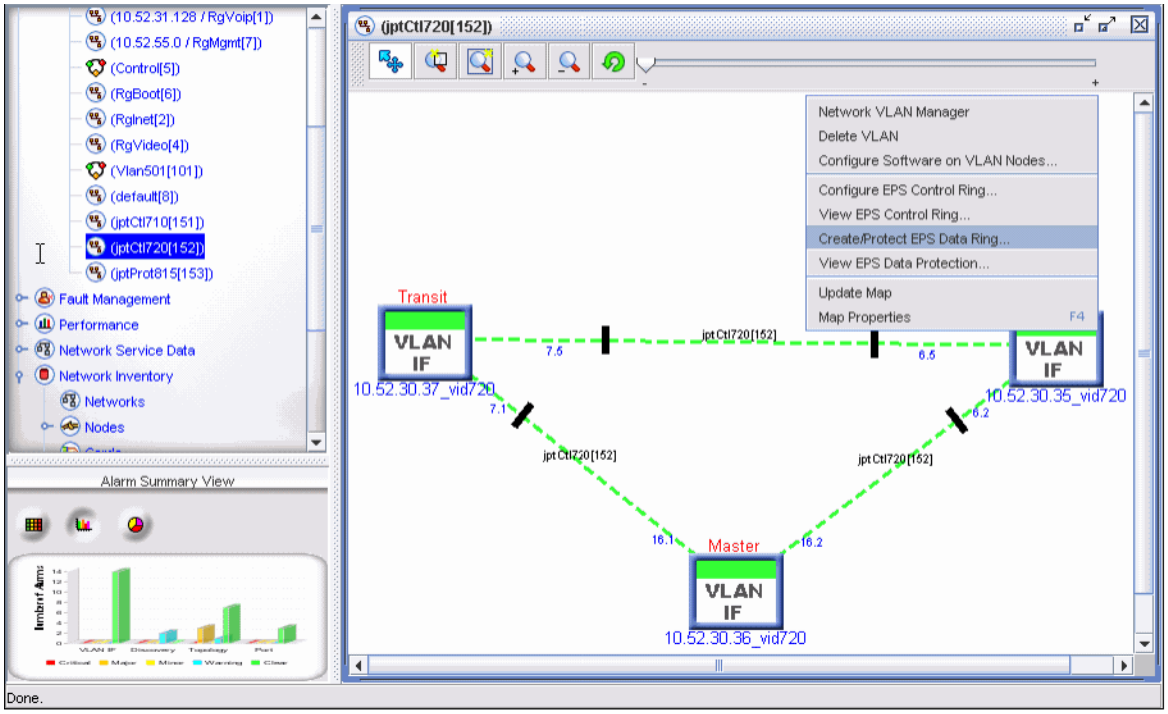
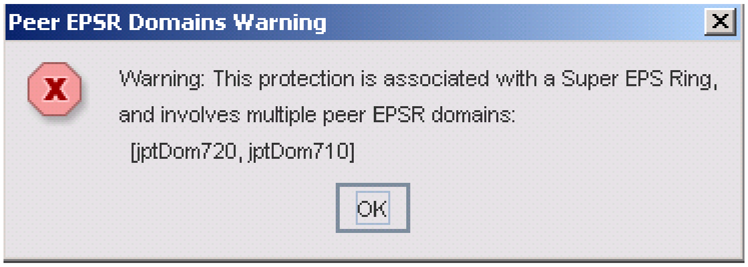


FIGURE 16-106 Creating Second Protected VLAN for SuperRing

A Warning is given to indicate that the data ring will be extended to multiple domains, as shown below.

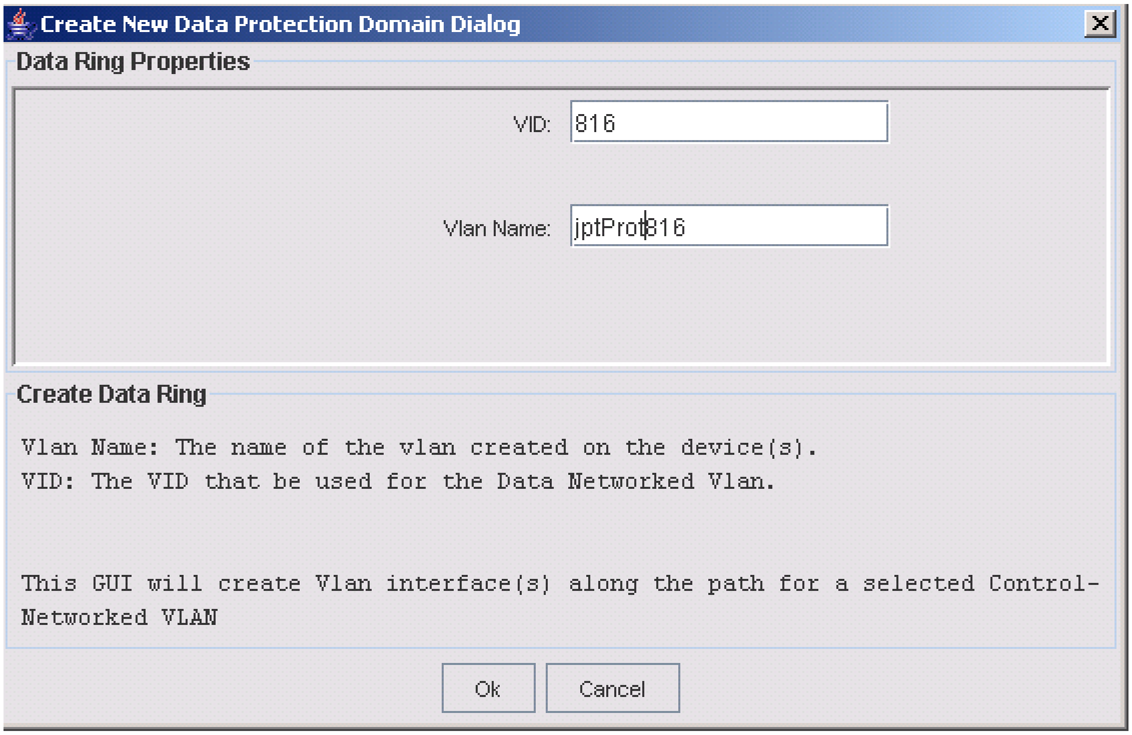


Peer EPSR Domains Warning

Warning: This protection is associated with a Super EPS Ring, and involves multiple peer EPSR domains:
[jptDom720, jptDom710]

FIGURE 16-107 Creating Second Protected VLAN for SuperRing - Warning

As with the first Protected VLAN, the GUIs lead the user through creating the second Protected VLAN. Note that the Protect Network VLAN Panel shows that all of the nodes of the SuperRing will have the VLAN added, as shown in the following figures.



Create New Data Protection Domain Dialog

Data Ring Properties

VID: 816

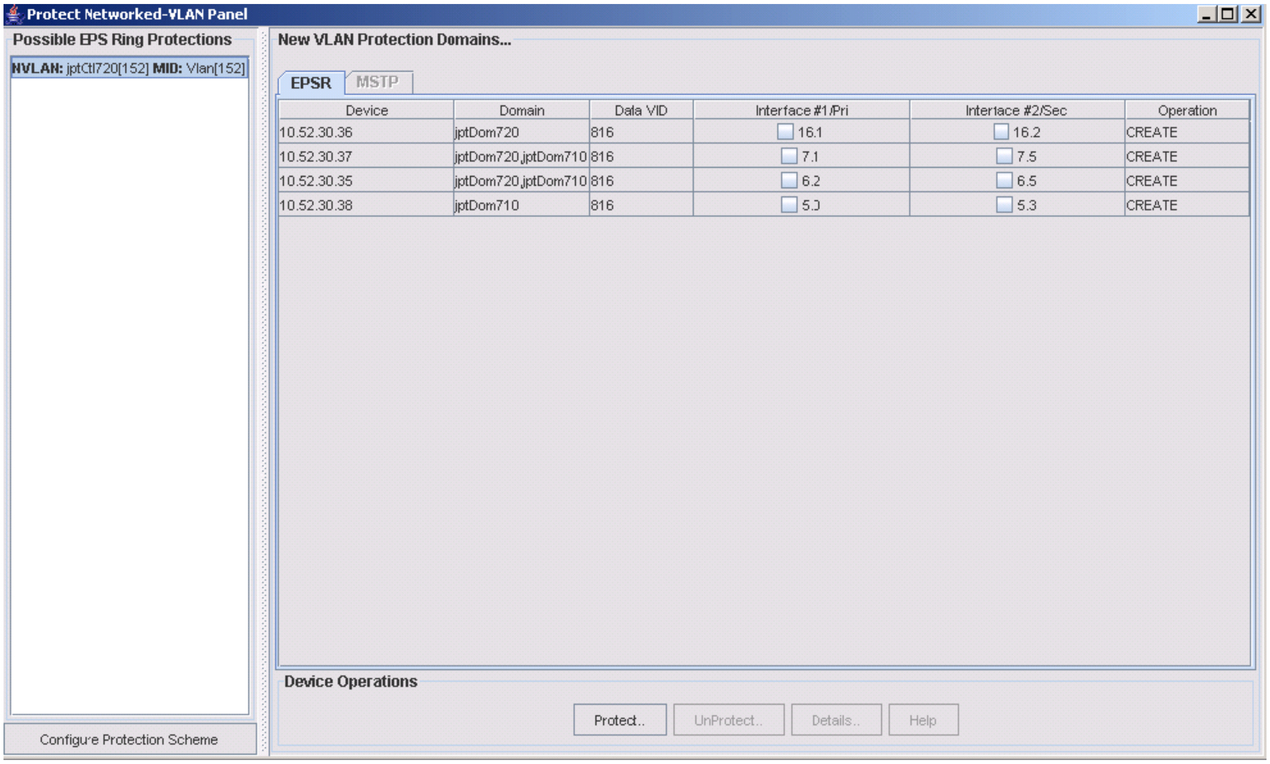
Vlan Name: jptProt816

Create Data Ring

Vlan Name: The name of the vlan created on the device(s).
VID: The VID that be used for the Data Networked Vlan.

This GUI will create Vlan interface(s) along the path for a selected Control-Networked VLAN

FIGURE 16-108 Creating Second Protected VLAN for SuperRing



Possible EPS Ring Protections

NVLAN: jptCtl720[152] **MID:** Vlan[152]

New VLAN Protection Domains...

Device	Domain	Data VID	Interface #1/Pri	Interface #2/Sec	Operation
10.52.30.36	jptDom720	816	□ 16.1	□ 16.2	CREATE
10.52.30.37	jptDom720,jptDom710	816	□ 7.1	□ 7.5	CREATE
10.52.30.35	jptDom720,jptDom710	816	□ 6.2	□ 6.5	CREATE
10.52.30.38	jptDom710	816	□ 5.3	□ 5.3	CREATE

Device Operations

FIGURE 16-109 Task List showing Protected VLAN extends to all Nodes in SuperRing

Selecting the Control VLAN in the left panel and then Configure Protection Scheme will take the Second Protected VLAN (816) and extend it over the entire SuperRing. When the Protected VLAN is created and the user clicks on the leaf for VLAN 816, all the nodes of the two EPS Rings are included, as shown in the following figure.

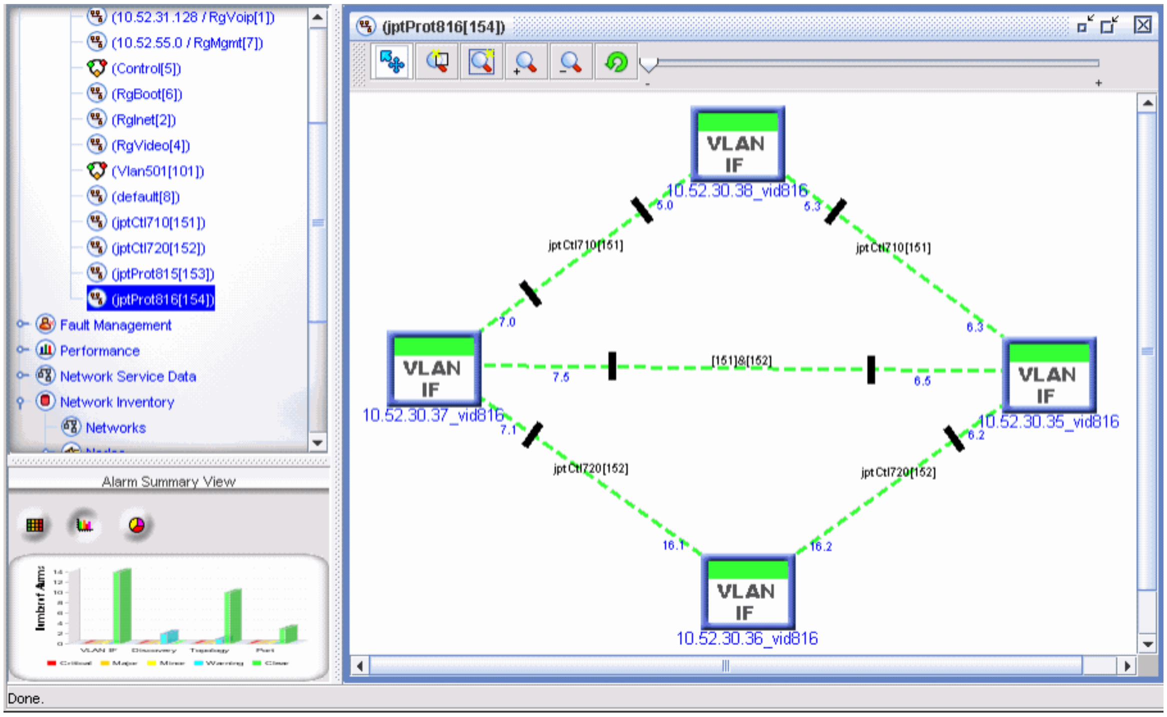
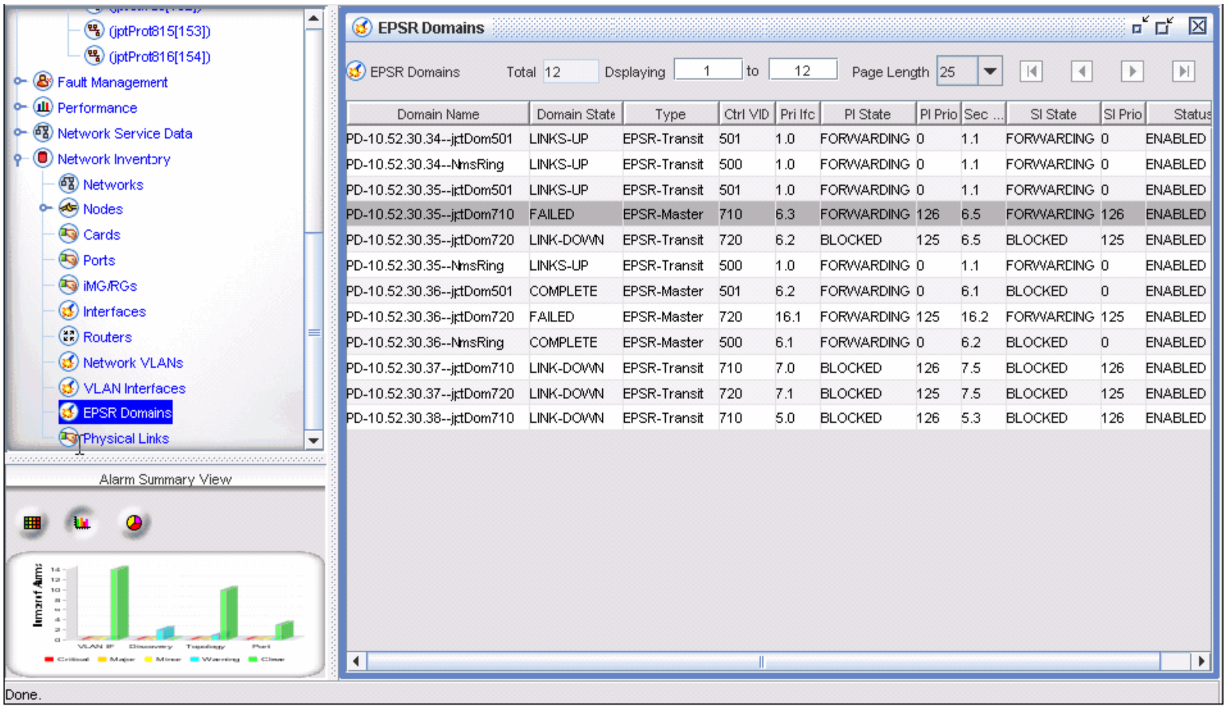


FIGURE 16-110 Protected VLAN across Multiple EPS Control VLANs (816)

16.11.2.6 Viewing Network Inventory

The Netwrok Inventory View shows the status of the SuperLoop, as shown in the following figure.



EPSR Domains

EPSR Domains Total 12 Dsplaying 1 to 12 Page Length 25

Domain Name	Domain State	Type	Ctrl VID	Pri Ifc	PI State	PI Prio	Sec ...	SI State	SI Prio	Status
PD-10.52.30.34--jptDom501	LINKS-UP	EPSR-Transit	501	1.0	FORWARDING	0	1.1	FORWARDING	0	ENABLED
PD-10.52.30.34--NmsRing	LINKS-UP	EPSR-Transit	500	1.0	FORWARDING	0	1.1	FORWARDING	0	ENABLED
PD-10.52.30.35--jptDom501	LINKS-UP	EPSR-Transit	501	1.0	FORWARDING	0	1.1	FORWARDING	0	ENABLED
PD-10.52.30.35--jptDom710	FAILED	EPSR-Master	710	6.3	FORWARDING	126	6.5	FORWARDING	126	ENABLED
PD-10.52.30.35--jptDom720	LINK-DOWN	EPSR-Transit	720	6.2	BLOCKED	125	6.5	BLOCKED	125	ENABLED
PD-10.52.30.35--NmsRing	LINKS-UP	EPSR-Transit	500	1.0	FORWARDING	0	1.1	FORWARDING	0	ENABLED
PD-10.52.30.36--jptDom501	COMPLETE	EPSR-Master	501	6.2	FORWARDING	0	6.1	BLOCKED	0	ENABLED
PD-10.52.30.36--jptDom720	FAILED	EPSR-Master	720	16.1	FORWARDING	125	16.2	FORWARDING	125	ENABLED
PD-10.52.30.36--NmsRing	COMPLETE	EPSR-Master	500	6.1	FORWARDING	0	6.2	BLOCKED	0	ENABLED
PD-10.52.30.37--jptDom710	LINK-DOWN	EPSR-Transit	710	7.0	BLOCKED	126	7.5	BLOCKED	126	ENABLED
PD-10.52.30.37--jptDom720	LINK-DOWN	EPSR-Transit	720	7.1	BLOCKED	125	7.5	BLOCKED	125	ENABLED
PD-10.52.30.38--jptDom710	LINK-DOWN	EPSR-Transit	710	5.0	BLOCKED	126	5.3	BLOCKED	126	ENABLED

FIGURE 16-111 Network Inventory for EPSR Domains

16.12 Customer Management

16.12.1 Overview

Provisioning services for customers usually involves setting the values of many parameters that vary depending on the type of service customers have requested, the service features to be provided, and the components to be configured. The Network Service applications available using the AlliedView NMS, such as Profiles and Quality of Service Policies, allow ports on the devices to be configured efficiently and without errors. The Customer Management feature allows individual customers to have their type of service configured, and incorporates these Network Service applications as well. This allows almost all customer attributes for any service to be included on one form.

Moreover, once one customer has been provisioned, these same attributes can be carried over in provisioning new customers, Finally, almost all attributes for a customer can be modified by selecting the **View/Modify Customer Ports** Form.

The following figure shows the options available. To access Customer Management, select *Tools -> Customer Management*.

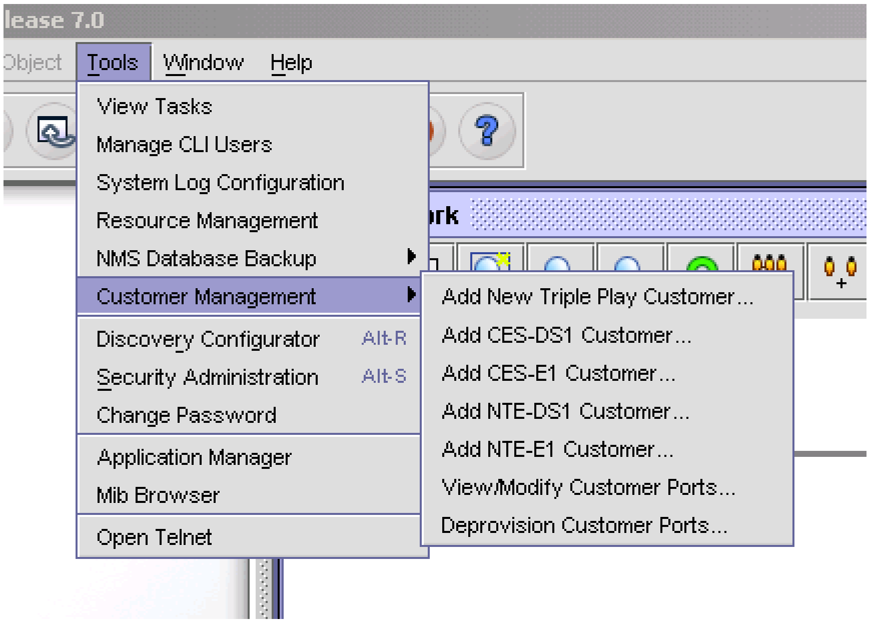


FIGURE 16-112 Accessing the Customer Management Options

16.12.2 Add New Triple Play Customer - Four Examples

The **Provision New Triple Play Customer** Form is used to provision on one form most of the attributes needed for one customer.

Note: *The fields of the Provision New Triple Play Customer Form are described in "Provision a New Triple Play Customer" on page 398.*

The form is divided into three main panels:

1. Video/Data Configuration
2. Voice Configuration
3. Derived Voice

Using this form is an efficient and error-free method to data fill a customer, and this becomes even more true when used in conjunction with profiles.

Figure 16-122 shows four example configurations for triple play

1. POTS24 for analog voice only - This is for an analog phone or modem.
2. POTS24 and ADSL for analog voice and video/data- This is using a Residential Gateway and the ADSL/POTS24 cards.
3. Ethernet - This is using a Residential Gateway and the FE10 card for digital voice and data/video
4. ADSL - This is for analog voice and data.

Following this figure are the **Provision New Triple Play Customer** Forms and how they would be filled out for each configuration.

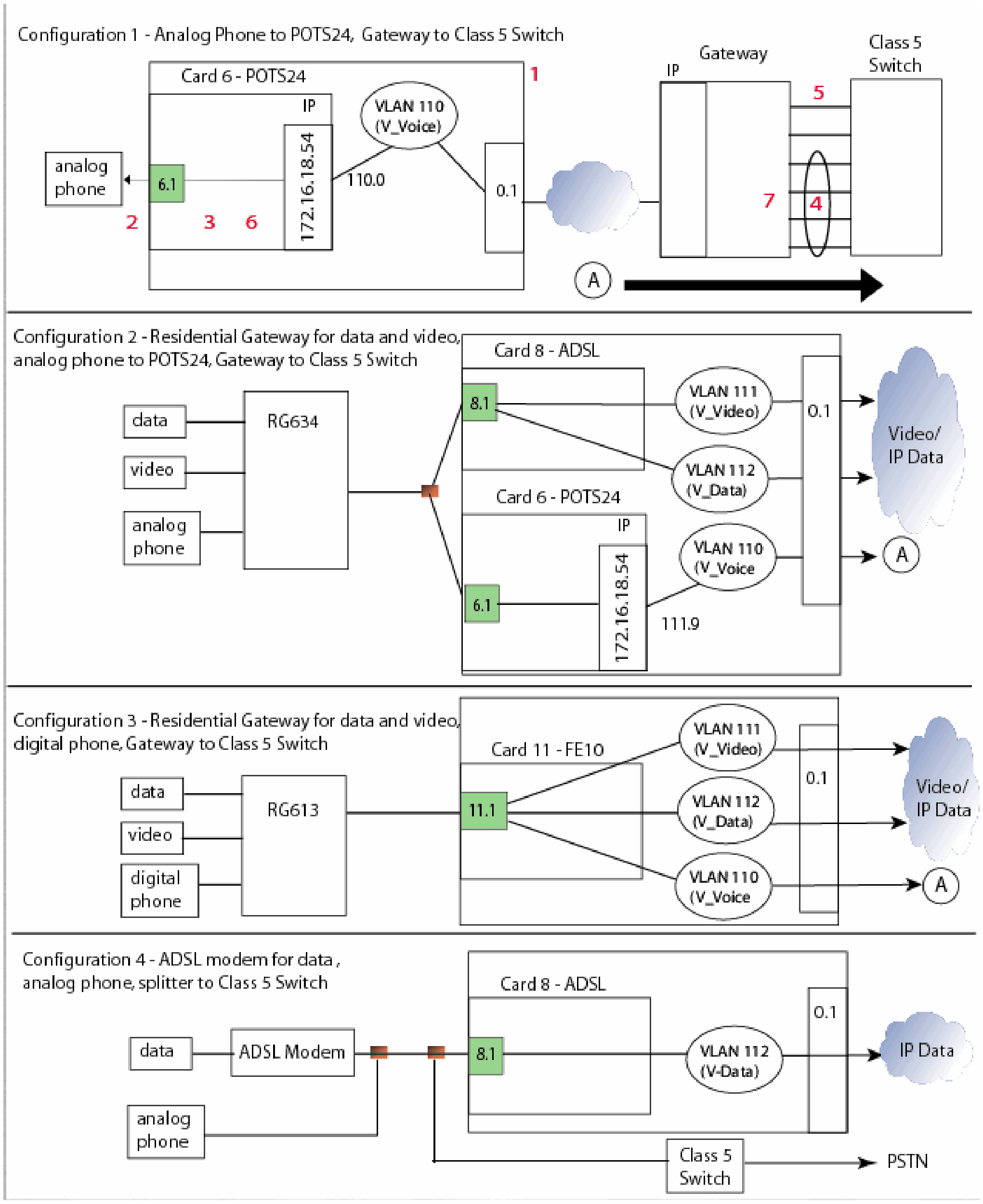
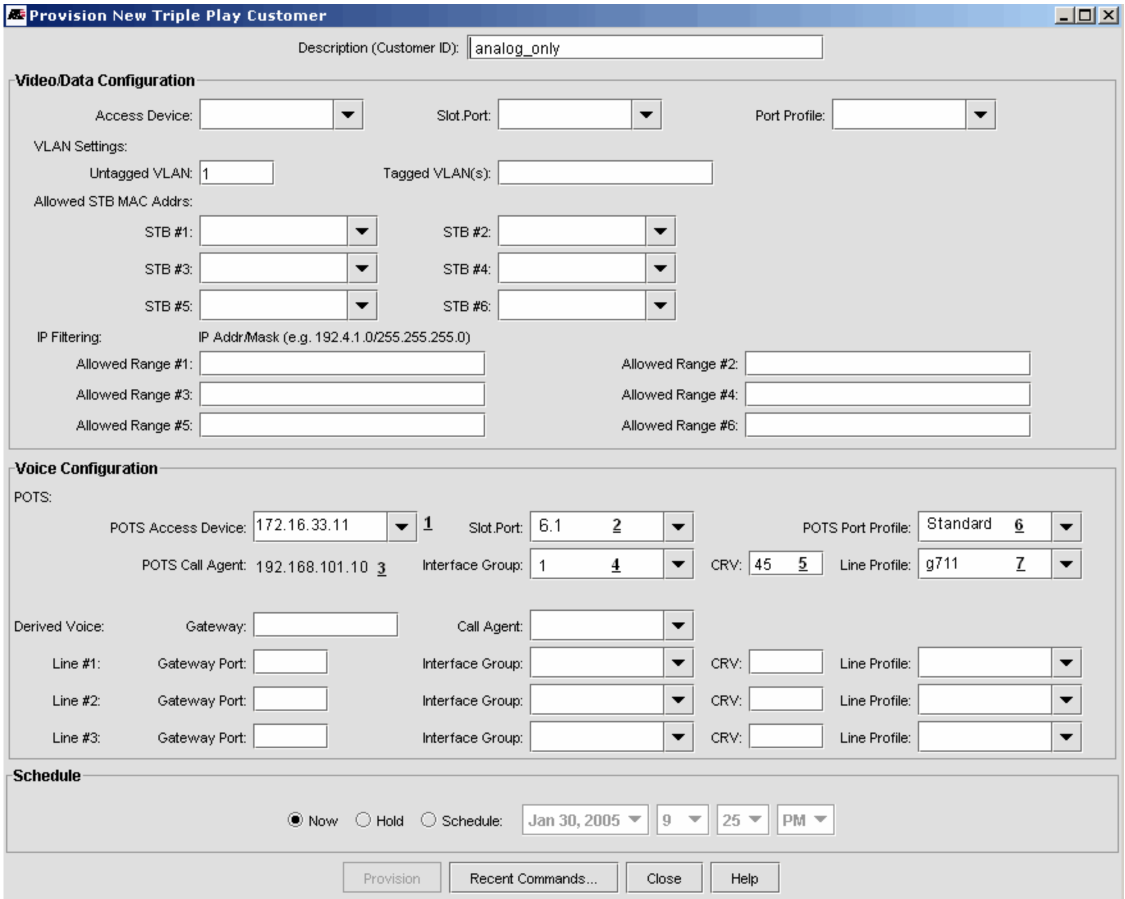


FIGURE 16-113 Four Example Configurations for Triple Play

16.12.2.1 Configuration 1 - POTS24 Only

In this scenario, only the middle panel (Voice Configuration) is filled in. The POTS Call Agent is filled in automatically when the POTS GW IP Addr. (the IP address for the POTS24 card) and the port is filled in. The Line Profile, a GW attribute, is available once the Gateway has been configured.

Note: In this figure, the underlined numbers in the fields match the Configuration 1 numbers in Figure 16-113.



Provision New Triple Play Customer

Description (Customer ID): analog_only

Untagged VLAN: 1

POTS Access Device: 172.16.33.11 1

Slot.Port: 6.1 2

POTS Port Profile: Standard 6

POTS Call Agent: 192.168.101.10 3

Interface Group: 1 4

CRV: 45 5

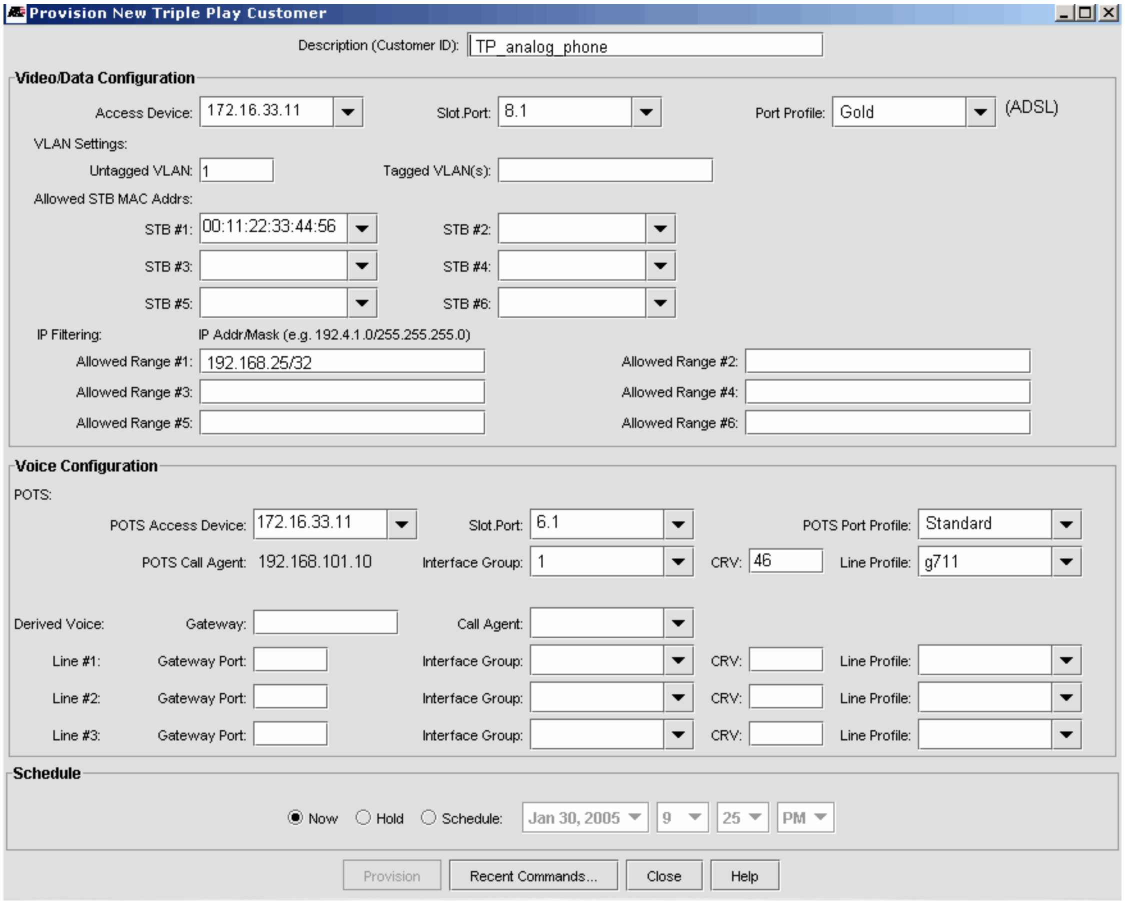
Line Profile: g711 7

● Now ○ Hold ○ Schedule: Jan 30, 2005 9 25 PM

FIGURE 16-114 Triple Play Form - POTS24 Only

16.12.2.2 Configuration 2 - POTS24 and ADSL Card, Analog Phone Only

In this configuration, an analog phone, data, and video are provided using an ADSL card and a separate POTS24 card that are combined using the Customer ID. (The POTS24 and ADSL card can be on separate systems if needed). The top and middle panels are filled in.



Provision New Triple Play Customer

Description (Customer ID): TP_analog_phone

Video/Data Configuration

Access Device: 172.16.33.11 Slot.Port: 8.1 Port Profile: Gold (ADSL)

VLAN Settings:

Untagged VLAN: 1 Tagged VLAN(s):

Allowed STB MAC Addrs:

STB #1: 00:11:22:33:44:56 STB #2:

STB #3: STB #4:

STB #5: STB #6:

IP Filtering: IP Addr/Mask (e.g. 192.4.1.0/255.255.255.0)

Allowed Range #1: 192.168.25/32 Allowed Range #2:

Allowed Range #3: Allowed Range #4:

Allowed Range #5: Allowed Range #6:

Voice Configuration

POTS:

POTS Access Device: 172.16.33.11 Slot.Port: 6.1 POTS Port Profile: Standard

POTS Call Agent: 192.168.101.10 Interface Group: 1 CRV: 46 Line Profile: g711

Derived Voice: Gateway: Call Agent:

Line #1: Gateway Port: Interface Group: CRV: Line Profile:

Line #2: Gateway Port: Interface Group: CRV: Line Profile:

Line #3: Gateway Port: Interface Group: CRV: Line Profile:

Schedule

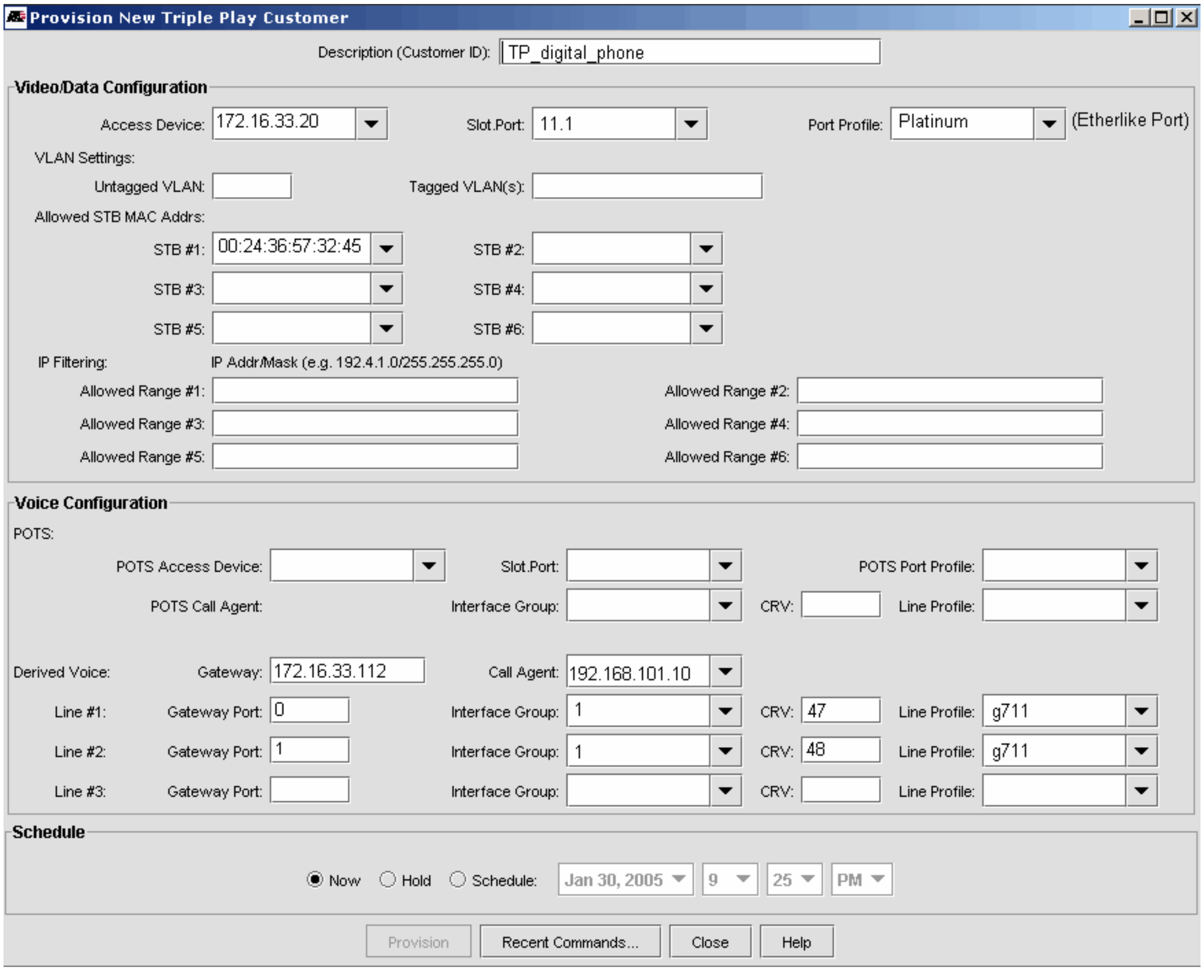
● Now ○ Hold ○ Schedule: Jan 30, 2005 9 25 PM

[

FIGURE 16-115 Triple Play Form - POTS24 and ADSL Card, Analog Phone Only

16.12.2.3 Configuration 3 - FE10 Card, Digital Phone Only, Video and Data

In this configuration, an iMAP 9000 is used, and using the FE card video and data are configured as well as a digital phone. The top and bottom panels are used, with the Gateway for the Derived Voice the IP Address on the Gateway Device.



Provision New Triple Play Customer

Description (Customer ID): TP_digital_phone

Video/Data Configuration

Access Device: 172.16.33.20 Slot.Port: 11.1 Port Profile: Platinum (Etherlike Port)

VLAN Settings:

Untagged VLAN: Tagged VLAN(s):

Allowed STB MAC Addrs:

STB #1: 00:24:36:57:32:45 STB #2:

STB #3: STB #4:

STB #5: STB #6:

IP Filtering: IP Addr/Mask (e.g. 192.4.1.0/255.255.255.0)

Allowed Range #1: Allowed Range #2:

Allowed Range #3: Allowed Range #4:

Allowed Range #5: Allowed Range #6:

Voice Configuration

POTS:

POTS Access Device: Slot.Port: POTS Port Profile:

POTS Call Agent: Interface Group: CRV: Line Profile:

Derived Voice: Gateway: 172.16.33.112 Call Agent: 192.168.101.10

Line #1: Gateway Port: 0 Interface Group: 1 CRV: 47 Line Profile: g711

Line #2: Gateway Port: 1 Interface Group: 1 CRV: 48 Line Profile: g711

Line #3: Gateway Port: Interface Group: CRV: Line Profile:

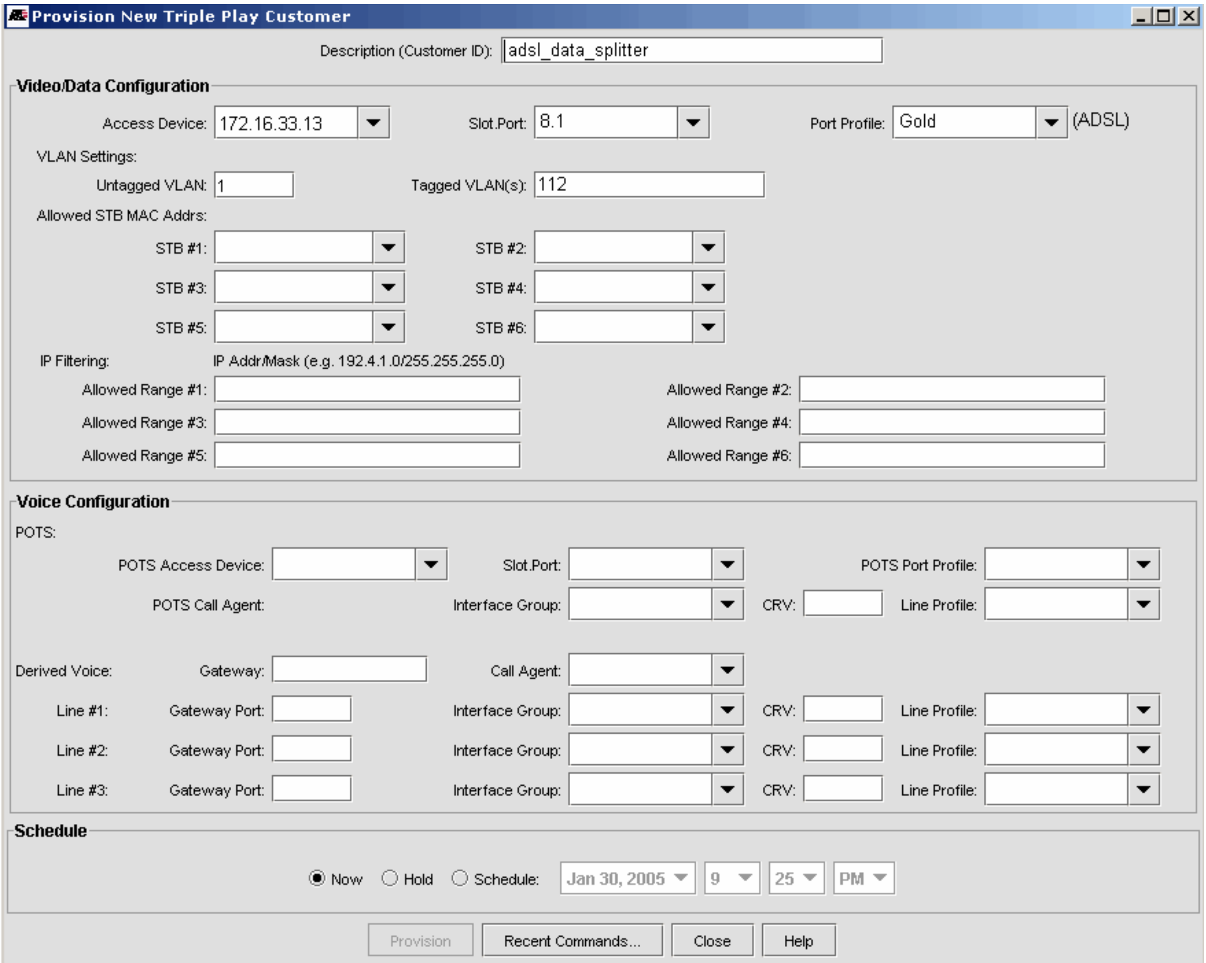
Schedule

● Now ○ Hold ○ Schedule: Jan 30, 2005 9 25 PM

FIGURE 16-116 FE10 Card, Digital Phone Only, Video and Data

16.12.2.4 Configuration 4 - ADSL for Data and Analog Phone with Splitter

In this configuration, only the top panel is filled out for the data service, since the phone service is split off from the iMAP device and goes to the Class 5 device.



Provision New Triple Play Customer

Description (Customer ID): adsl_data_splitter

Video/Data Configuration

Access Device: 172.16.33.13
Slot.Port: 8.1
Port Profile: Gold (ADSL)

VLAN Settings:
Untagged VLAN: 1
Tagged VLAN(s): 112

Schedule: ● Now ○ Hold ○ Schedule: Jan 30, 2005 9 25 PM

FIGURE 16-117 ADSL for Data, Analog Phone with Splitter

16.12.3 Add DS1/E1 Customer

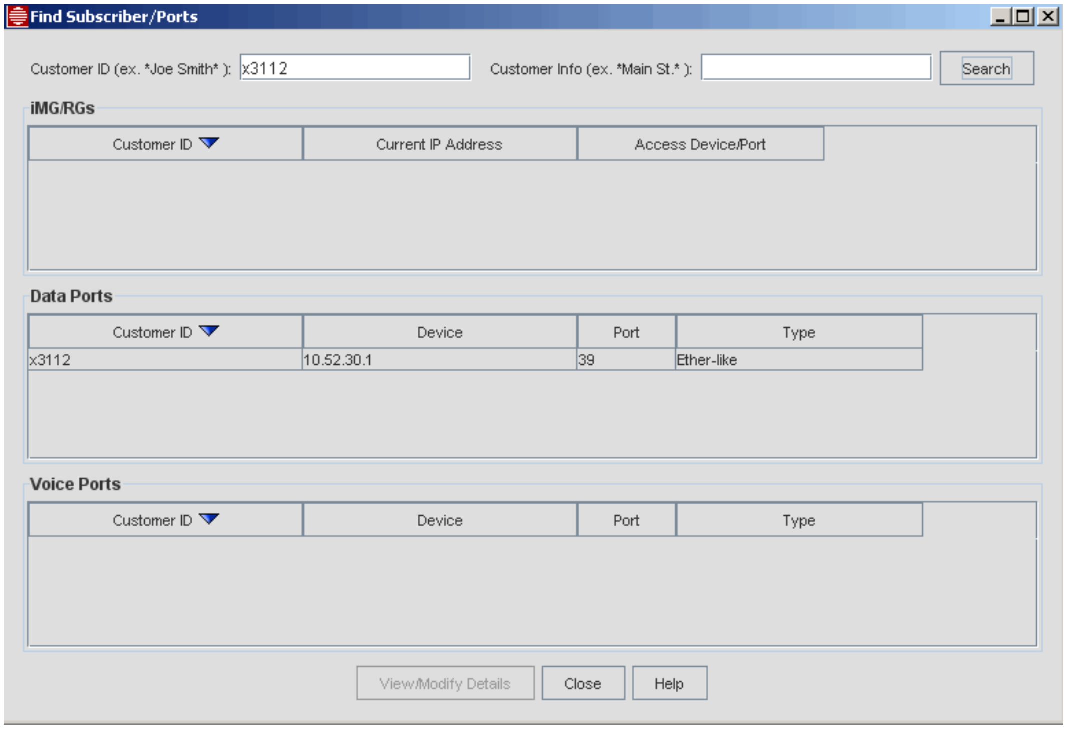
This is part of provisioning a CES customer, and brings up the Provision New DS1/E1 Port Form. The fields on this form are explained in "Provision New CES8-DS1 Port Form" on page 403. A configuration with example values is shown in "Create/ Provision CES8 card to Support DS1 Ports (Same Device)" on page 625.

16.12.4 View/Modify Customer Ports

The **Find Subscriber/Ports Form** is a powerful tool that allows the user to search, display, and change customer port attributes, and can help highlight when a Customer ID name is not appropriate.

To access the Find Subscriber/Ports Form, select from the main menu *Tools -> Customer Management -> View/Modify Customer Ports*. The Find Subscriber/Ports Form appears. Input a Customer ID, and the associated port(s) appear, as shown in the following figure.

Note: The "" can be used as a wild card to search for customer IDs that match patterns.*



Customer ID (ex. *Joe Smith*): x3112

Customer Info (ex. *Main St.*):

iMG/RGs

Customer ID	Current IP Address	Access Device/Port

Data Ports

Customer ID	Device	Port	Type
x3112	10.52.30.1	39	Ether-like

Voice Ports

Customer ID	Device	Port	Type

FIGURE 16-118 Find Subscriber/Ports Form

Once the port(s) appear, the user can either double-click a port or select the port and click on **View/Modify Details** to bring up the relevant Port Management Form, where attributes can be viewed and modified.

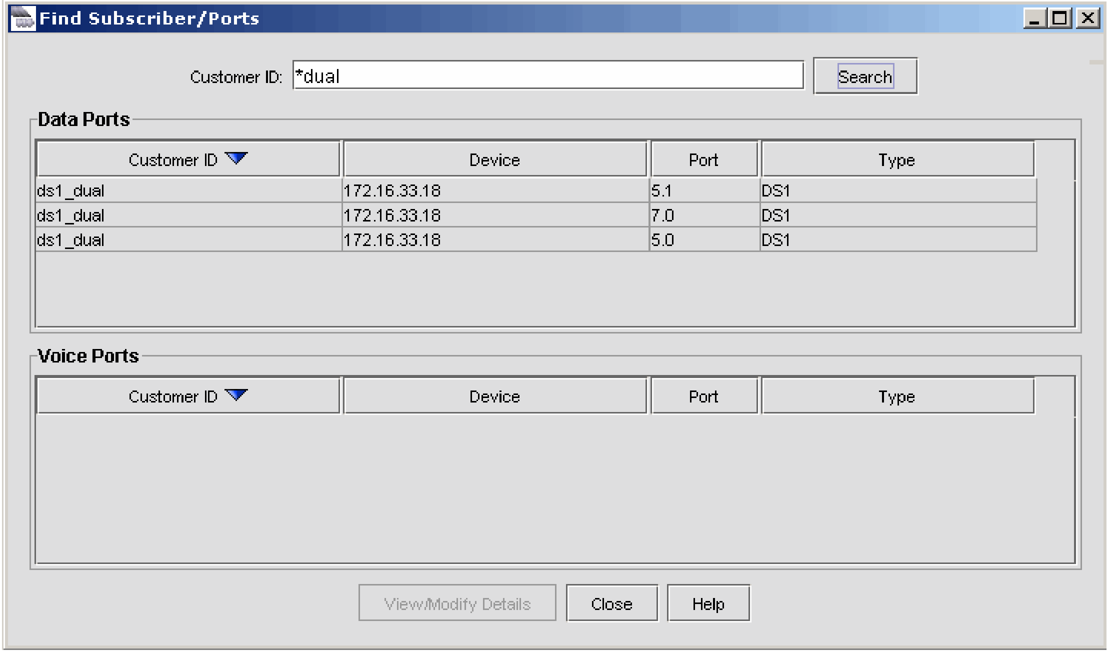
Note: The View/Modify Details button is enabled when one entry is selected.

By searching on the Customer ID, the user can quickly find the relevant services/ports that are being used for a customer and can quickly view the current attributes and make any changes.

Caution: Customer IDs should be unique and should apply to one customer line. The one exception is with the dual CES configuration, explained below.

Proper use of a customer ID is important because it helps the administrator understand how the services/ports have been configured. For example, in a CES dual endpoint configuration (explained in "Circuit Emulation Service" on page 623), each DS1 port has the same customer ID or label. In the following figure, the name for each endpoint is ds1_dual. However, a third DS1 endpoint has also been given the customer ID of ds1_dual, so one of the ports is not part of the dual endpoint configuration. By viewing the details of each port and looking at the actual values for each one (especially the IP and UDP values at the PSPAN level), the user can determine which ports are actually connected and then rename the third DS1 port to something more appropriate.

It is possible that all three DS1 ports could have been single endpoints, but the purpose of the customer ID is to use names that match the configuration and therefore allow easy recognition of what the customer has.



Customer ID: *dual

Data Ports

Customer ID	Device	Port	Type
ds1_dual	172.16.33.18	5.1	DS1
ds1_dual	172.16.33.18	7.0	DS1
ds1_dual	172.16.33.18	5.0	DS1

Voice Ports

Customer ID	Device	Port	Type

FIGURE 16-119 Ambiguous Use of Customer ID

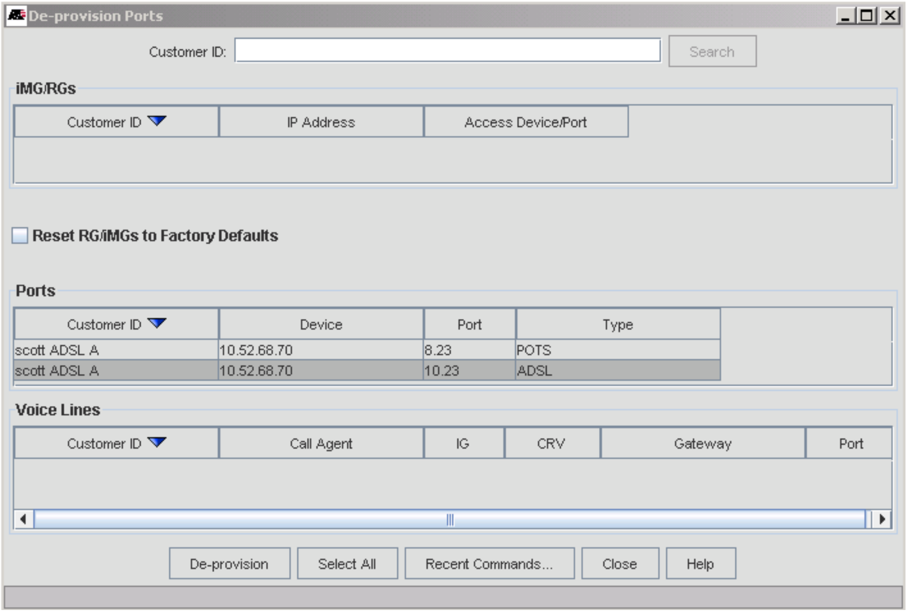
16.12.5 Deprovision Customer Ports

This form allows the user to quickly find the ports/voice lines associated with a subscriber ID and deprovision them.

Note: *This form can also be accessed from the Port Inventory or Port Management main screen by right-clicking on the relevant port and selecting De-Provision Customer/Port.*

After selecting the appropriate ports/lines, the user can deprovision the port/line immediately or at a scheduled time. The figures blow show the following:

- A customer that has both an ADSL and POTS card provisioned. The ports are shown in the Ports panel while the associated Voice Lines are shown in the Voice Lines Panel.
- A dual-endpoint CES connection. Note that the use of the Customer ID is correct, as the one ID is used to identify the two (and only two) associated ports.



Customer ID:

iMG/RGs

Customer ID	IP Address	Access Device/Port

□ Reset RG/iMGs to Factory Defaults

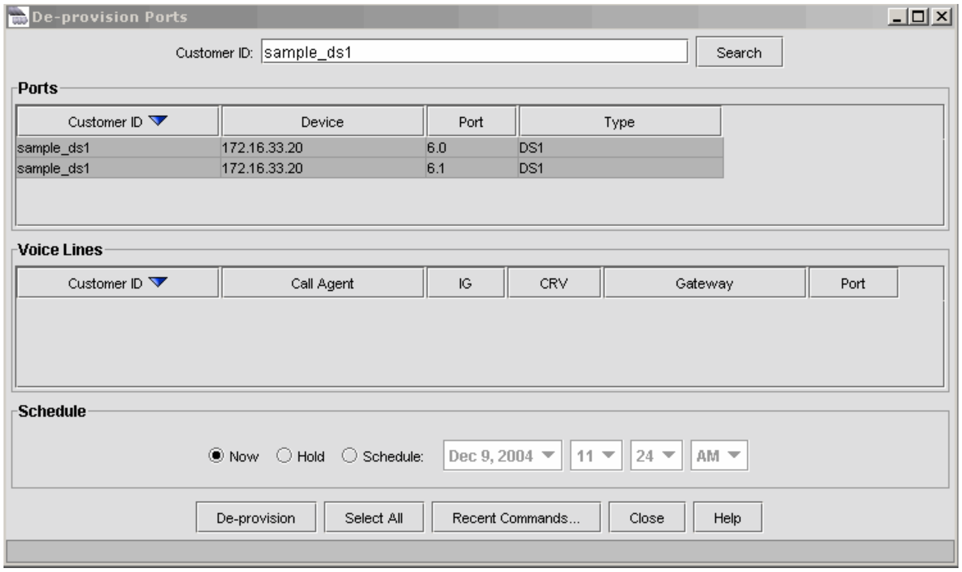
Ports

Customer ID	Device	Port	Type
scott ADSL A	10.52.68.70	8.23	POTS
scott ADSL A	10.52.68.70	10.23	ADSL

Voice Lines

Customer ID	Call Agent	IG	CRV	Gateway	Port

FIGURE 16-120 De-provision Ports Form - ADSL/POTS



Customer ID: sample_ds1

Ports

Customer ID	Device	Port	Type
sample_ds1	172.16.33.20	6.0	DS1
sample_ds1	172.16.33.20	6.1	DS1

Voice Lines

Customer ID	Call Agent	IG	CRV	Gateway	Port

Schedule

● Now ○ Hold ○ Schedule: Dec 9, 2004 11 24 AM

FIGURE 16-121 De-provision Ports Form - DS1 Endpoints (CES)

16.13 Circuit Emulation Service

16.13.1 CES8 and iMG6x6MOD Configurations

Circuit Emulation is a service that is provided by Allied Telesis using the following:

- CES8 card - The CES8 card is used to provide “Pass-thru” Circuit Emulation Service for both E1 and DS1 circuits

Note: Refer to "CES8 Card" on page 387 and "CES8 Port (DS1/E1 Port Management Tabbed Form)" on page 456 for an overview of the CES8 card and DS1/E1 port attributes.

The CES configuration can be either single or dual port; in a dual port configuration both ends of the CES circuit are iMAP DS1/E1 ports managed by the NMS, while in a single port configuration, only one DS1/E1 port is configured on an iMAP device managed by the NMS.

- iMG6x6MOD - With the iMG6x6MOD, a circuit emulation service can also be provided. The DS1/E1 port on the iMG can connect to either a CES8 card or another iMG6x6MOD.

The first part of this section will focus on the CES8 to CES8 card configurations, and includes connections between CES8 cards on the same iMAP as well as different iMAPs.

The second part of this section will focus on the iMG6x6MOD and highlights an iMG6x6MOD with connections to ports on the CES8 card, with one port to the public voice switching and the other to a PBX/Channel Bank.

16.13.2 CES8 Configuration - Overview of Steps

The steps for provisioning the CES ports are basically the same regardless of whether single or dual port is being configured:

1. Create the Card (this includes provisioning all ports as DS1 or E1) - Refer to "Create/Provision CES8 card to Support DS1 Ports (Same Device)" on page 625
2. Add the IP interface to the card (this includes the VLAN)
3. Create the port profile - Refer to "Create DS1 Profile (DS1 and P-SPAN)" on page 626
4. Provision the port - This will also provision the PSPAN and connect the PSPAN to the port. - Refer to "Provision the Two DS1 Ports" on page 627

The following figure shows an example configuration using DS1 ports. (E1 ports are similar.) The detailed steps show how the forms are used.

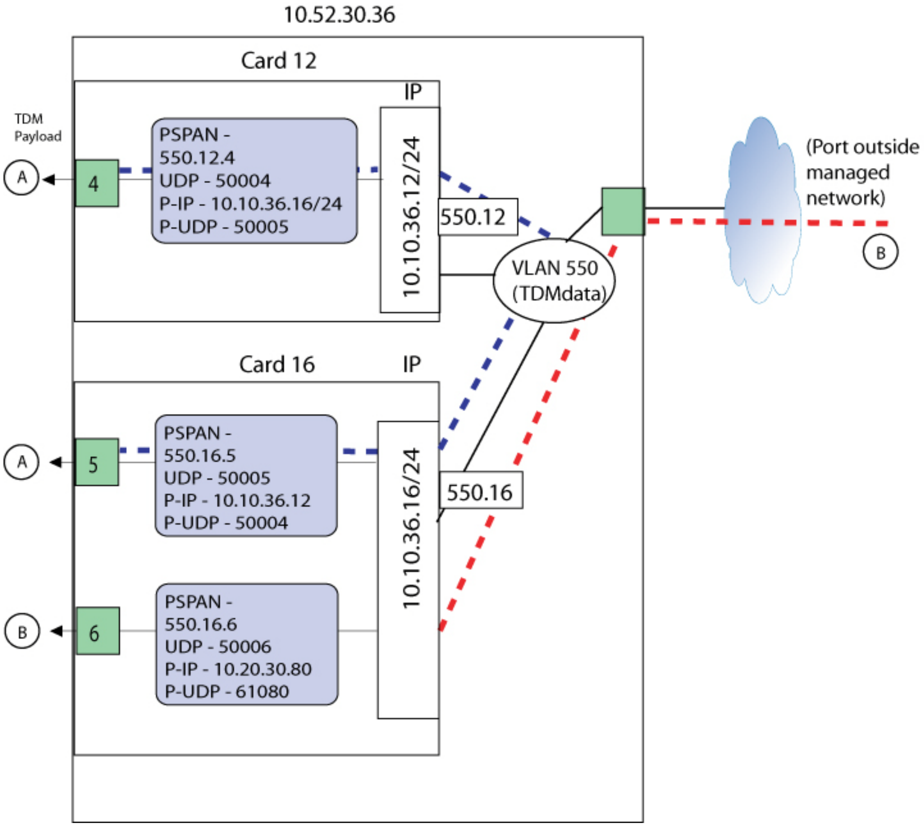


FIGURE 16-122 CES8 Card Configuration

16.13.3 Create/Provision CES8 card to Support DS1 Ports (Same Device)

The following steps are followed to create a connection between two ports on different cards in the **same** device, In Figure 16-122, this would be the A to A connection. (The B to B connection is for a port that is connected to a port that is outside the managed network.)

Note: The two ports can also be on different devices in the same managed network.

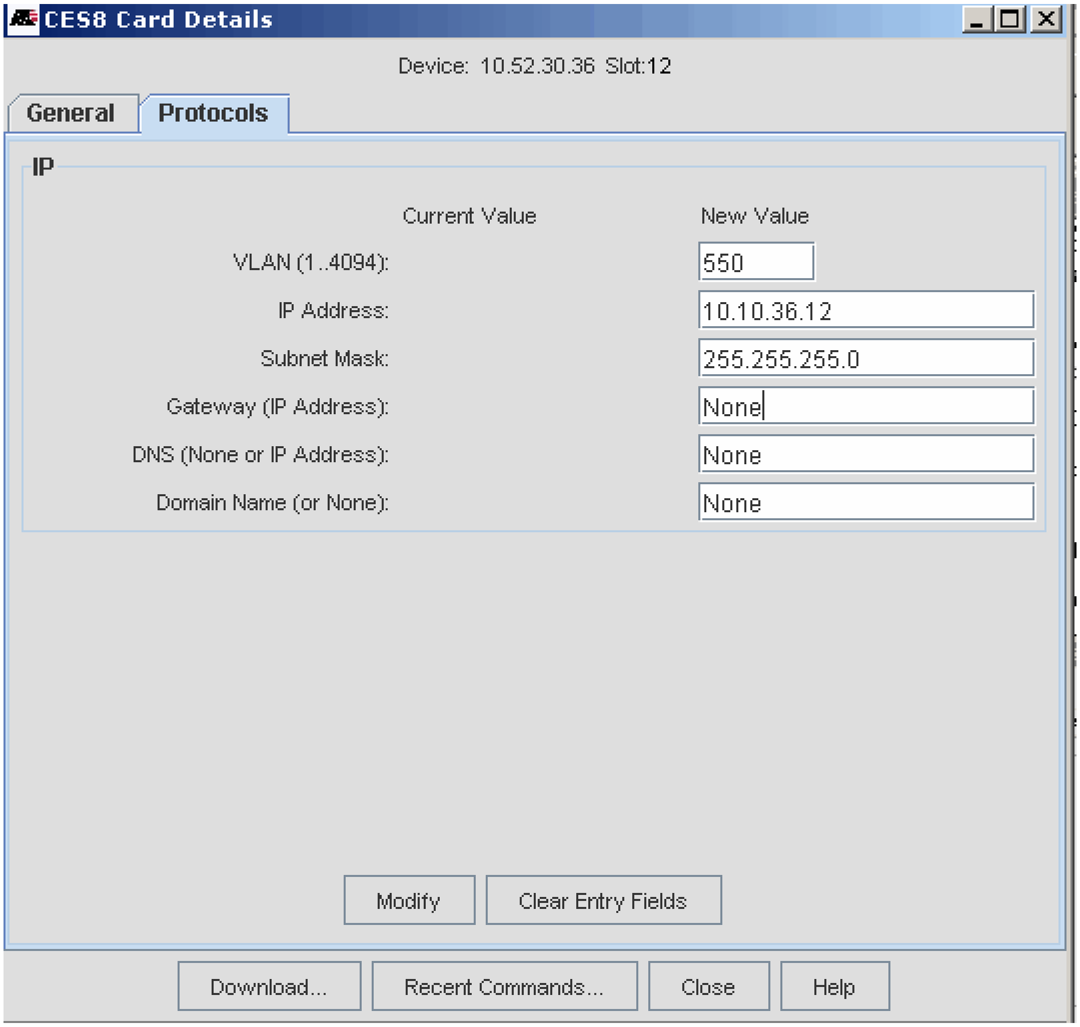
To create the cards (if this hasn't been done already), go to the **Card Management Form**, find the Slot (in this case 12) that is not provisioned, and select **Create Card**. Select the Profile as AutoProv if you wish the card to use the load that is in the AutoProv profile, the Admin State as UP (assuming you want the card to go into service), and the Ports Type as DS1. Click on **Create**, and the card status will change in the Card Management form to a Card Type of CES8.

At this point you can download any CES8 files if the Profile was set to Manually Provisioned.

To provision the IP interface, select the card and View Details, and in the CES8 Card Details Form, select the Protocols tab. Fill in the required VLAN, IP Address, and Subnet Mask fields, and the optional fields if needed. Select Modify and the values are applied.

The following figure shows the card on device 10.52.30.36, slot 12, with the values filled for the Protocols tab.

The same procedure is repeated for the card in slot 16.



Device: 10.52.30.36 Slot:12

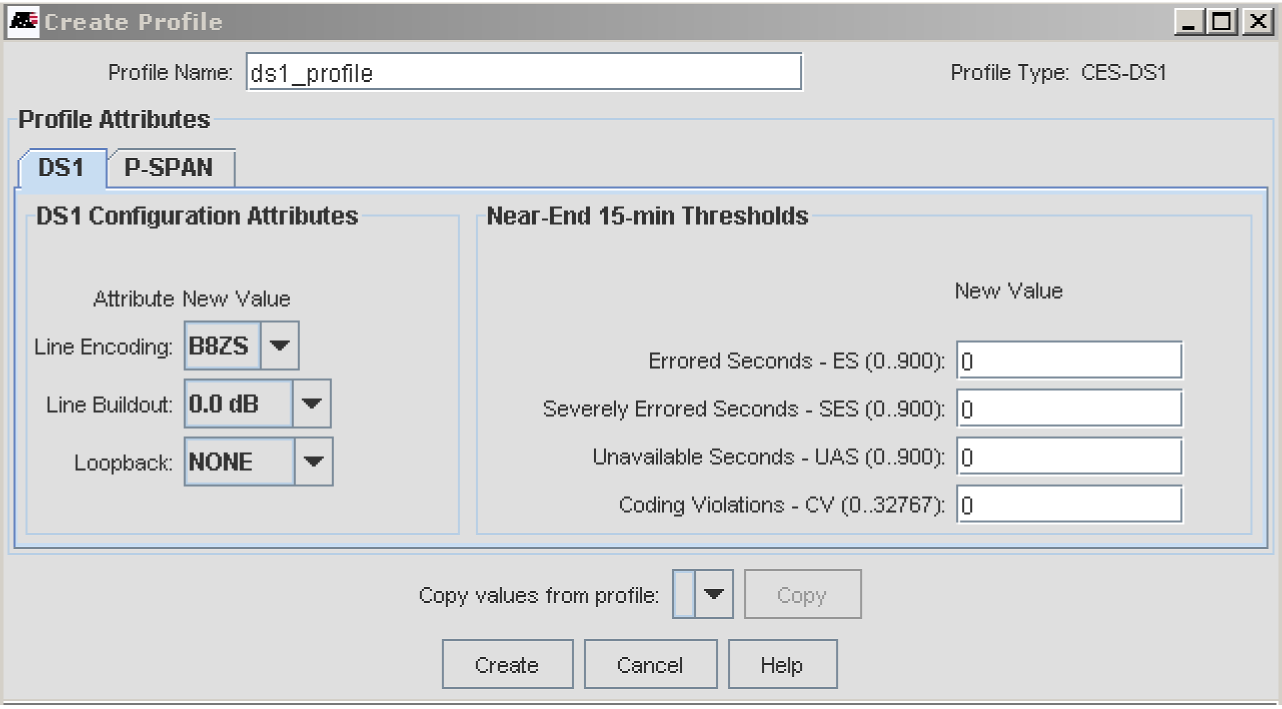
	Current Value	New Value
VLAN (1..4094):		550
IP Address:		10.10.36.12
Subnet Mask:		255.255.255.0
Gateway (IP Address):		None
DNS (None or IP Address):		None
Domain Name (or None):		None

FIGURE 16-123 Setting the IP Interface for the CES8 Card

Note: At this point, the card attribute Ports Type for the General Tab can be changed, but the card would need to be disabled, and there is a warning about the need to disable the card. The Profile can also be changed, and there is a warning that such a change will destroy existing provisioning data.

16.13.4 Create DS1 Profile (DS1 and P-SPAN)

When a DS1 port is provisioned, a DS1 profile must already exist so it can be associated with the DS1 port. In this example a profile called ds1_profile is created. The following figures show creating the profile. (Once created, they can be viewed in the Profile table by double-clicking on the profile row.)



Profile Name: ds1_profile

Profile Type: CES-DS1

Line Encoding: B8ZS

Line Buildout: 0.0 dB

Loopback: NONE

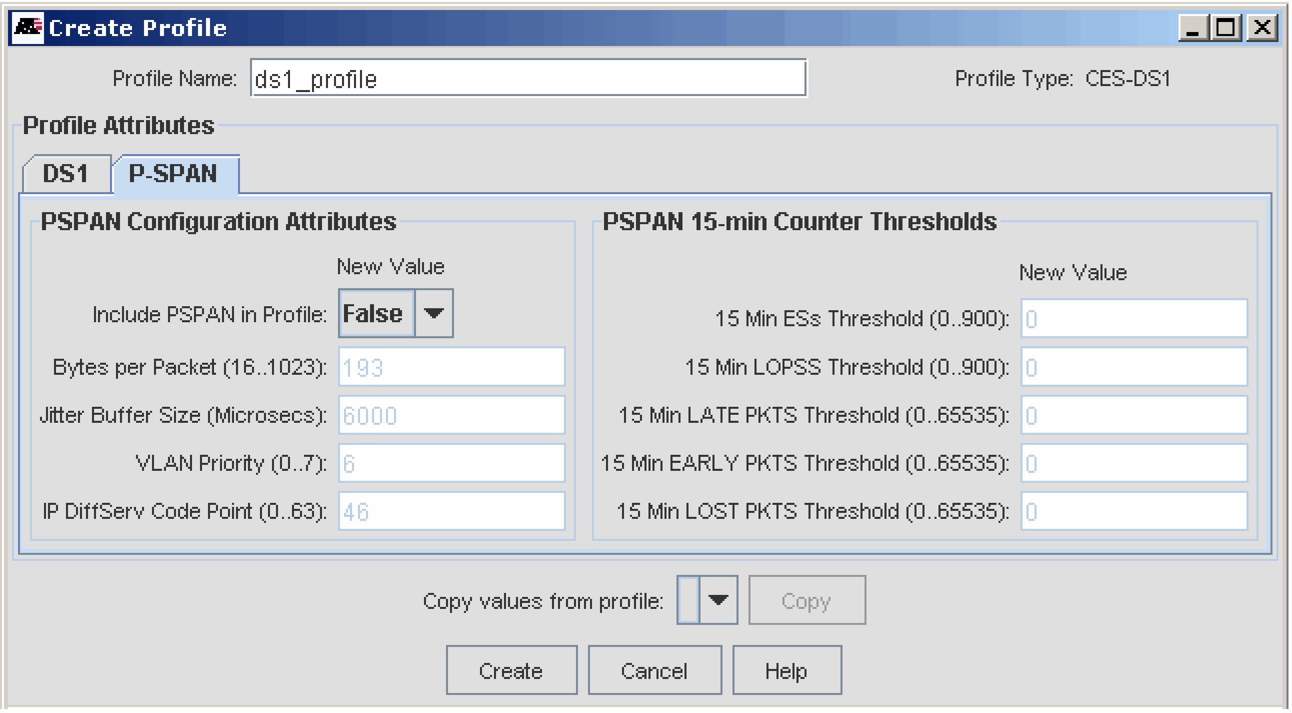
Errored Seconds - ES (0..900): 0

Severely Errored Seconds - SES (0..900): 0

Unavailable Seconds - UAS (0..900): 0

Coding Violations - CV (0..32767): 0

FIGURE 16-124 Creating a DS1 Profile (DS1 tab)



Profile Name: ds1_profile

Profile Type: CES-DS1

PSPAN Configuration Attributes

	New Value
Include PSPAN in Profile:	False
Bytes per Packet (16..1023):	193
Jitter Buffer Size (Microsecs):	6000
VLAN Priority (0..7):	6
IP DiffServ Code Point (0..63):	46

PSPAN 15-min Counter Thresholds

	New Value
15 Min ESs Threshold (0..900):	0
15 Min LOPSS Threshold (0..900):	0
15 Min LATE PKTS Threshold (0..65535):	0
15 Min EARLY PKTS Threshold (0..65535):	0
15 Min LOST PKTS Threshold (0..65535):	0

Copy values from profile:

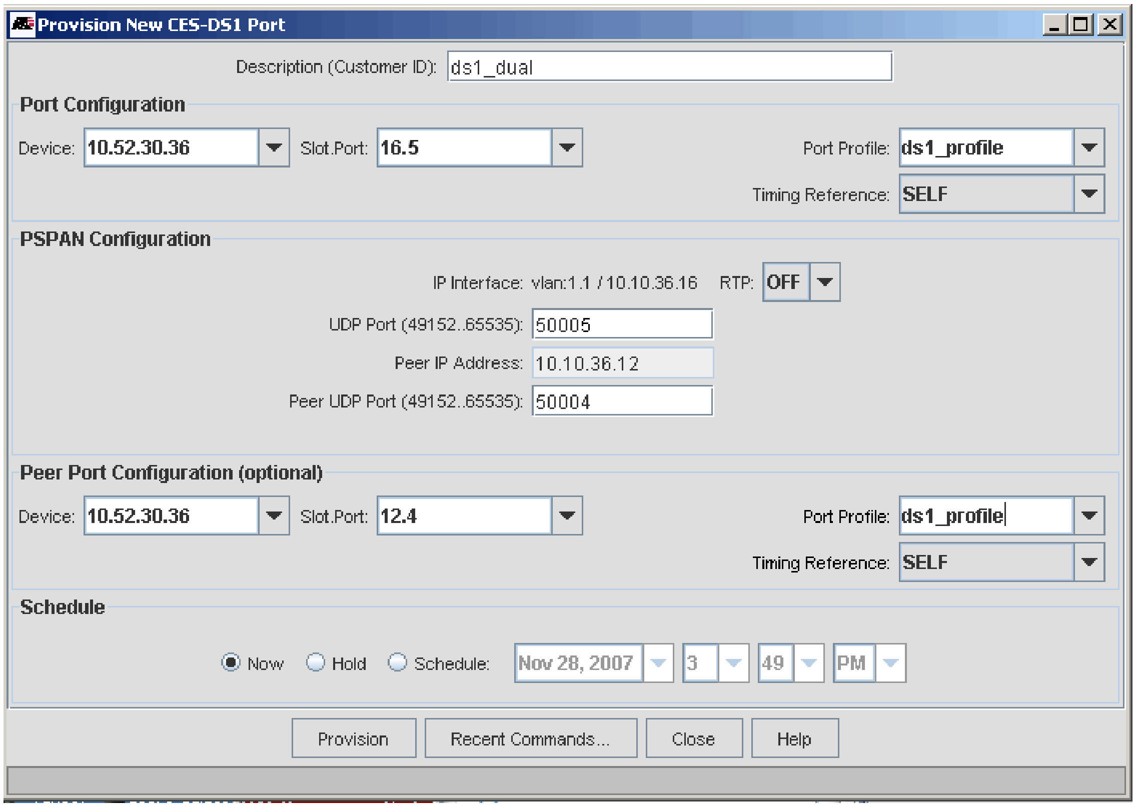
FIGURE 16-125 Creating a DS1 Profile (PSPAN tab)

Note: *If the user has already defined PSPAN Configuration Attributes and Counter Thresholds at the iMAP, the default for these in the Profile is set to False (read only), so they will not be affected. Otherwise, the user could define them here.*

16.13.5 Provision the Two DS1 Ports

Selecting from the main menu *Tools -> Customer Management -> Add DS1 Customer* brings up the **Provision New DS1 Port** Form. This is the form where the main tasks for Provisioning the CES8 endpoint and the PSPAN are done. The device/ports available are the discovered DS1 ports in the managed network that are available for provisioning. Following are important points when filling out this form:

- You must input a Customer ID. When provisioning two endpoints, this ID will be applied to both endpoints in the Port Inventory table. This allows immediate recognition of which ports are included in the dual configuration. The name should be descriptive so that the user can identify the customer that owns the DS1 circuit.
- When you enter a peer port device, the Peer IP Address of the first endpoint is automatically filled in and is uneditable. (If only one port is being provisioned, leave the Peer Port Configuration panel empty. The Peer IP address in the PSPAN Configuration panel will then be editable.)
- The Port Profiles used for each endpoint do not have to match, but their PSPAN tab parameters must be compatible.
- When a DS1 port is successfully provisioned, there is an option to provision another port, in which case the Customer ID field is cleared, and the just provisioned ports are no longer available in the Port pull-down.



Description (Customer ID): ds1_dual

Port Configuration

Device: 10.52.30.36 Slot.Port: 16.5 Port Profile: ds1_profile

Timing Reference: SELF

PSPAN Configuration

IP Interface: vlan:1.1 / 10.10.36.16 RTP: OFF

UDP Port (49152..65535): 50005

Peer IP Address: 10.10.36.12

Peer UDP Port (49152..65535): 50004

Peer Port Configuration (optional)

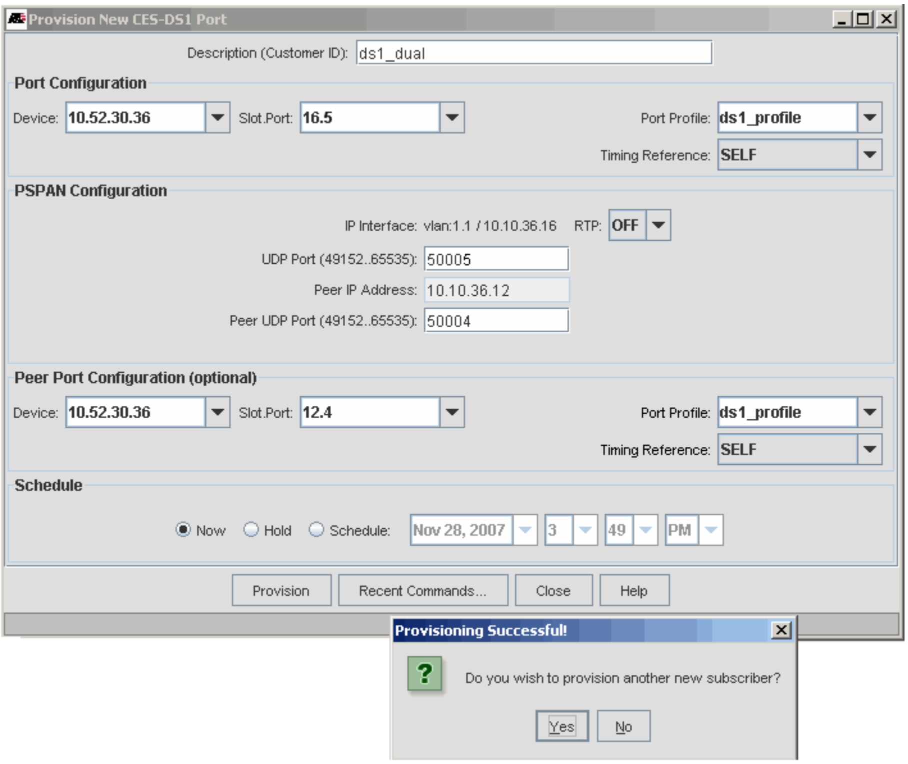
Device: 10.52.30.36 Slot.Port: 12.4 Port Profile: ds1_profile

Timing Reference: SELF

Schedule

● Now ○ Hold ○ Schedule: Nov 28, 2007 3 49 PM

FIGURE 16-126 Provision a New DS1 Port (Dual Points)



Description (Customer ID): ds1_dual

Port Configuration

Device: 10.52.30.36 Slot.Port: 16.5 Port Profile: ds1_profile

Timing Reference: SELF

PSPAN Configuration

IP Interface: vlan:1.1 / 10.10.36.16 RTP: OFF

UDP Port (49152..65535): 50005

Peer IP Address: 10.10.36.12

Peer UDP Port (49152..65535): 50004

Peer Port Configuration (optional)

Device: 10.52.30.36 Slot.Port: 12.4 Port Profile: ds1_profile

Timing Reference: SELF

Schedule

● Now ○ Hold ○ Schedule: Nov 28, 2007 3 49 PM

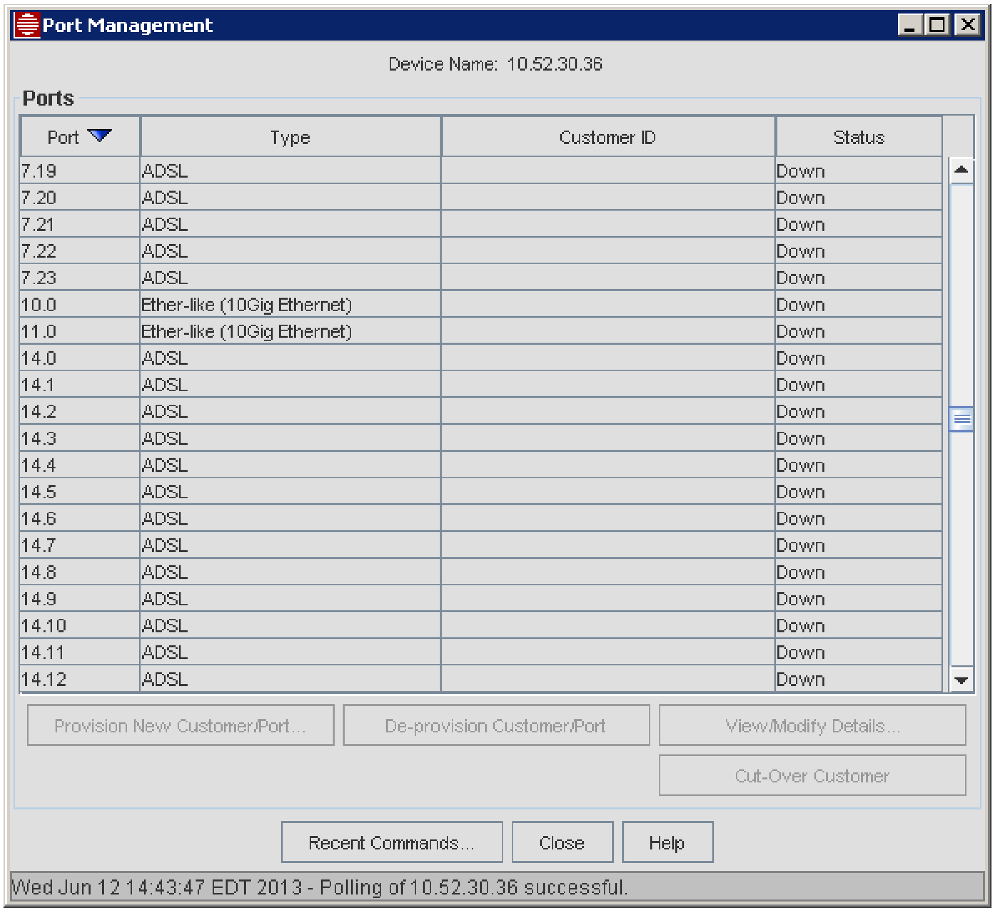
Provisioning Successful!

Do you wish to provision another new subscriber?

FIGURE 16-127 Result of Success (Fields Ready for next Customer)

16.13.6 View Provisioning Results

To see the results of the dual endpoint provisioning, go to the Port Management window for the device and sort on Customer ID. Refer to the following figure.



Port	Type	Customer ID	Status
7.19	ADSL		Down
7.20	ADSL		Down
7.21	ADSL		Down
7.22	ADSL		Down
7.23	ADSL		Down
10.0	Ether-like (10Gig Ethernet)		Down
11.0	Ether-like (10Gig Ethernet)		Down
14.0	ADSL		Down
14.1	ADSL		Down
14.2	ADSL		Down
14.3	ADSL		Down
14.4	ADSL		Down
14.5	ADSL		Down
14.6	ADSL		Down
14.7	ADSL		Down
14.8	ADSL		Down
14.9	ADSL		Down
14.10	ADSL		Down
14.11	ADSL		Down
14.12	ADSL		Down

Wed Jun 12 14:43:47 EDT 2013 - Polling of 10.52.30.36 successful.

FIGURE 16-128 Viewing Dual Endpoints - Same Customer ID

This shows that ports 12.4 and 16.5 are the endpoints. By double-clicking on either of these rows, the DS1 Port Management tabbed form appears, and one can view/modify the details of the configuration.

Note: *In this tabbed form, it is possible to change the attributes of the endpoints, and even to split the dual endpoints into two single endpoints, if that is desired. However, in most cases the user should plan the dual endpoints so that configuration is easy and less prone to error.*

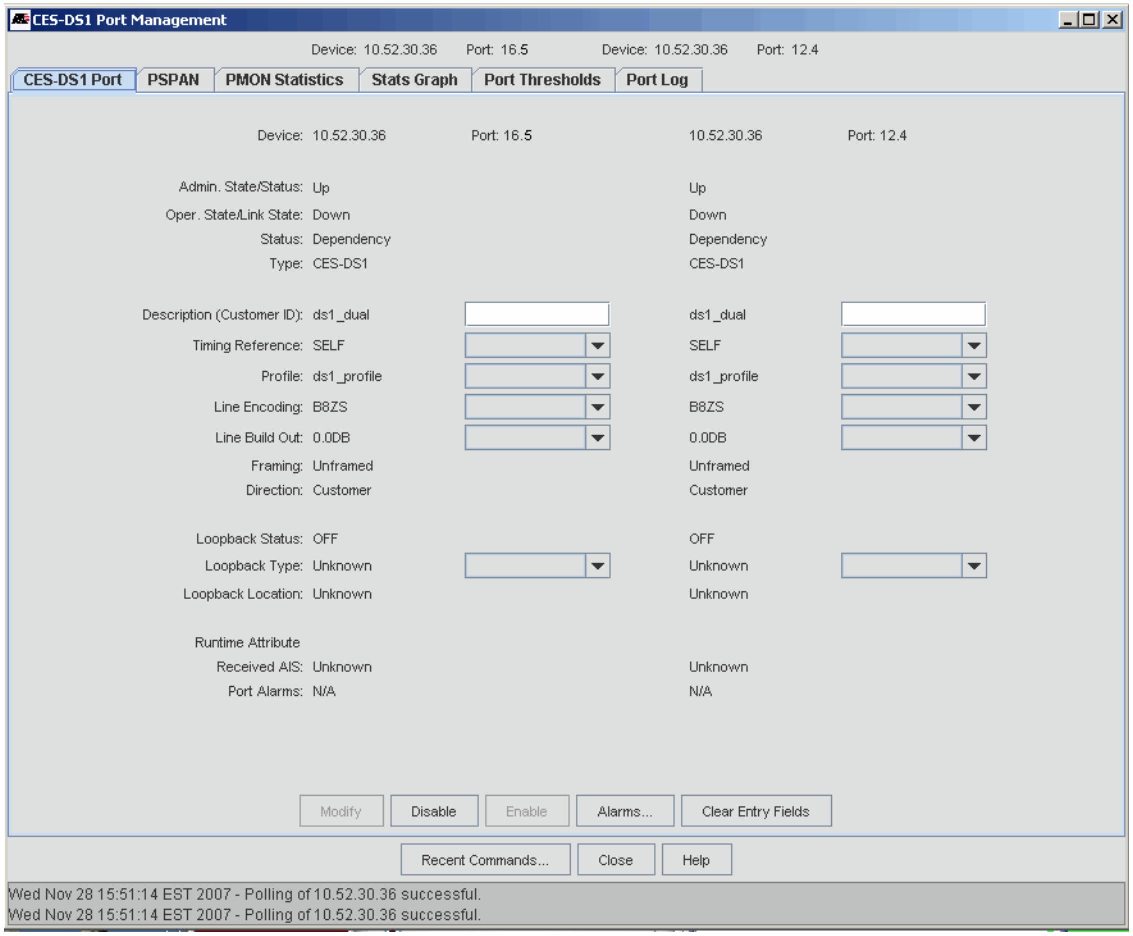
16.13.6.1 DS1 Port Tab

The following figure shows the form that appears when the user double-clicks on port 16.5.

The port 16.5 is on the left, since that is the row that was selected; if the user selected 12.4, port 12.4 would appear on the left.

The user can change attributes that are part of the Profile, but after clicking on Modify the user would see the Profile with an "*" next to it, meaning the Profile is out-of-sync. (This would also show up in the port inventory table.) The user would need to re-apply the profile to make the '*' disappear.

Note: The DS1 tab shows only the implicit connection between the endpoints; it is the PSPAN tab that explicitly ties the two endpoints together, discussed below.



Device: 10.52.30.36 Port: 16.5 Device: 10.52.30.36 Port: 12.4

Device:	10.52.30.36 Port: 16.5	10.52.30.36 Port: 12.4
Admin. State/Status:	Up	Up
Oper. State/Link State:	Down	Down
Status:	Dependency	Dependency
Type:	CES-DS1	CES-DS1
Description (Customer ID):	ds1_dual	ds1_dual
Timing Reference:	SELF	SELF
Profile:	ds1_profile	ds1_profile
Line Encoding:	B8ZS	B8ZS
Line Build Out:	0.0DB	0.0DB
Framing:	Unframed	Unframed
Direction:	Customer	Customer
Loopback Status:	OFF	OFF
Loopback Type:	Unknown	Unknown
Loopback Location:	Unknown	Unknown
Runtime Attribute		
Received AIS:	Unknown	Unknown
Port Alarms:	N/A	N/A

```
Wed Nov 28 15:51:14 EST 2007 - Polling of 10.52.30.36 successful.
Wed Nov 28 15:51:14 EST 2007 - Polling of 10.52.30.36 successful.
```

FIGURE 16-129 Viewing Dual CES points - DS1 Port Tab

16.13.6.2 PSPAN Tab

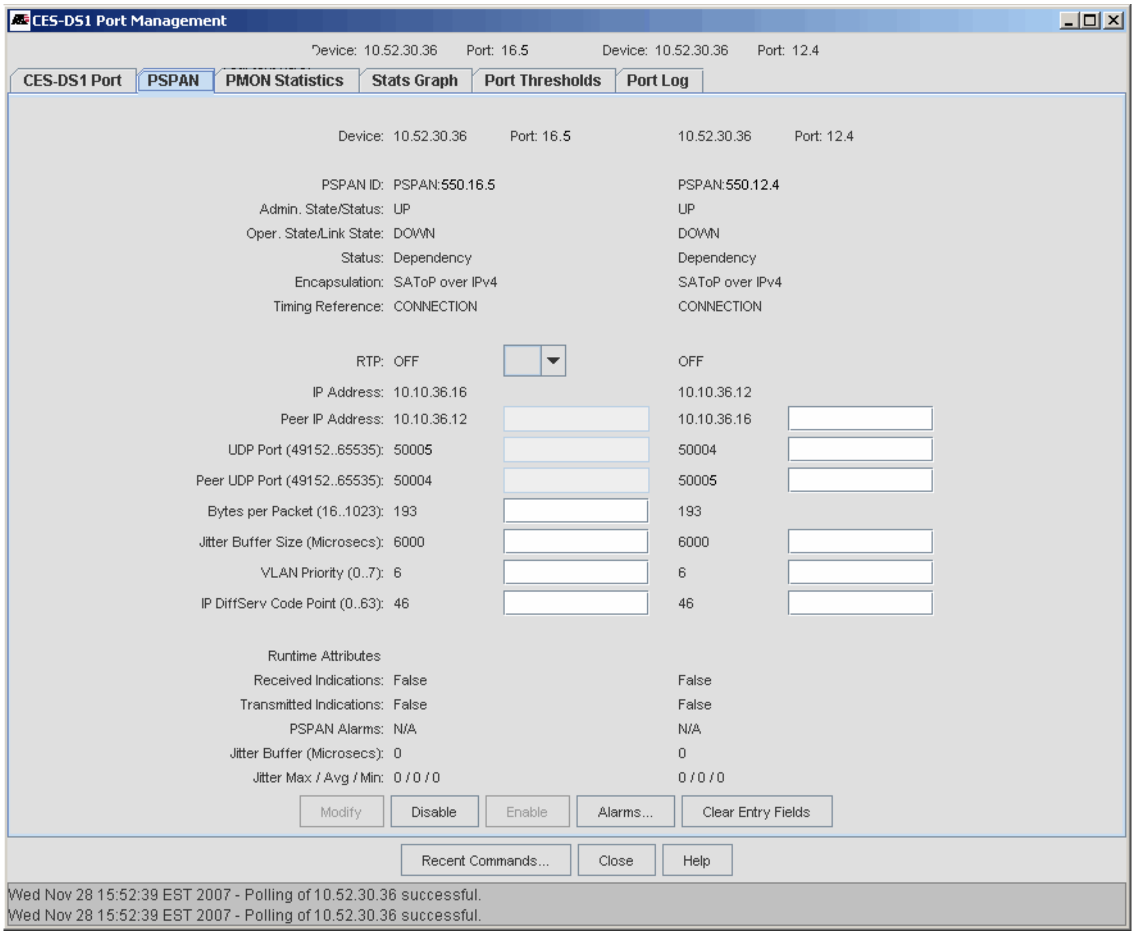
The following figure shows the PSPAN tab for the two endpoints.

As with the DS1 tab, the row selected is the port that appears on the left.

The main attributes of the PSPANs are at the top of the form and are read only.

The editable attributes are at the bottom of the form. Note, however, that the Peer IP Address and Peer UDP Port are read only since this is a two-port configuration. (In a one-port configuration, these fields are editable.)

Changing the RTP for one PSPAN changes it for both PSPANs to keep them compatible.



Device: 10.52.30.36 Port: 16.5 Device: 10.52.30.36 Port: 12.4

Device:	10.52.30.36 Port: 16.5	10.52.30.36 Port: 12.4
PSPAN ID:	PSPAN:550.16.5	PSPAN:550.12.4
Admin. State/Status:	UP	UP
Oper. State/Link State:	DOWN	DOWN
Status:	Dependency	Dependency
Encapsulation:	SAToP over IPv4	SAToP over IPv4
Timing Reference:	CONNECTION	CONNECTION
RTP:	OFF	OFF
IP Address:	10.10.36.16	10.10.36.12
Peer IP Address:	10.10.36.12	10.10.36.16
UDP Port (49152..65535):	50005	50004
Peer UDP Port (49152..65535):	50004	50005
Bytes per Packet (16..1023):	193	193
Jitter Buffer Size (Microsecs):	6000	6000
VLAN Priority (0..7):	6	6
IP DiffServ Code Point (0..63):	46	46
Runtime Attributes		
Received Indications:	False	False
Transmitted Indications:	False	False
PSPAN Alarms:	N/A	N/A
Jitter Buffer (Microsecs):	0	0
Jitter Max / Avg / Min:	0 / 0 / 0	0 / 0 / 0

```
Wed Nov 28 15:52:39 EST 2007 - Polling of 10.52.30.36 successful.
Wed Nov 28 15:52:39 EST 2007 - Polling of 10.52.30.36 successful.
```

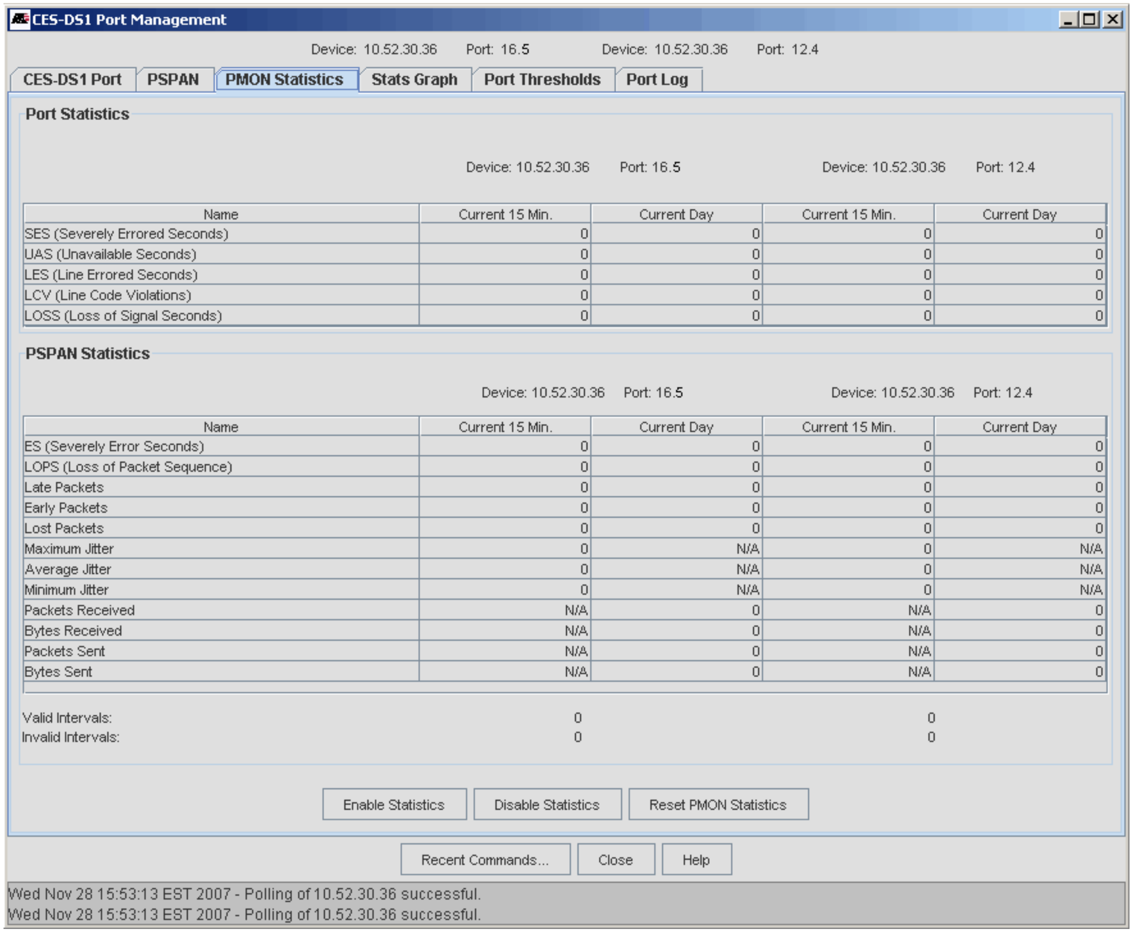
FIGURE 16-130 Viewing Dual CES points - PSPAN Tab

16.13.6.3 PMON Statistics Tab

This tab shows the PMON Statistics tab. Refer to the following figure.

Note that the table lists the 16.5 and 12.4 Port and PSPAN statistics together.

When the user presses the function buttons (Enable, Disable, etc.), they are applied to **both** ports.



Device: 10.52.30.36 Port: 16.5 Device: 10.52.30.36 Port: 12.4

Port Statistics

Device: 10.52.30.36 Port: 16.5 Device: 10.52.30.36 Port: 12.4

Name	Current 15 Min.	Current Day	Current 15 Min.	Current Day
SES (Severely Errored Seconds)	0	0	0	0
UAS (Unavailable Seconds)	0	0	0	0
LES (Line Errored Seconds)	0	0	0	0
LCV (Line Code Violations)	0	0	0	0
LOSS (Loss of Signal Seconds)	0	0	0	0

PSPAN Statistics

Device: 10.52.30.36 Port: 16.5 Device: 10.52.30.36 Port: 12.4

Name	Current 15 Min.	Current Day	Current 15 Min.	Current Day
ES (Severely Error Seconds)	0	0	0	0
LOPS (Loss of Packet Sequence)	0	0	0	0
Late Packets	0	0	0	0
Early Packets	0	0	0	0
Lost Packets	0	0	0	0
Maximum Jitter	0	N/A	0	N/A
Average Jitter	0	N/A	0	N/A
Minimum Jitter	0	N/A	0	N/A
Packets Received	N/A	0	N/A	0
Bytes Received	N/A	0	N/A	0
Packets Sent	N/A	0	N/A	0
Bytes Sent	N/A	0	N/A	0

Valid Intervals:	0	0
Invalid Intervals:	0	0

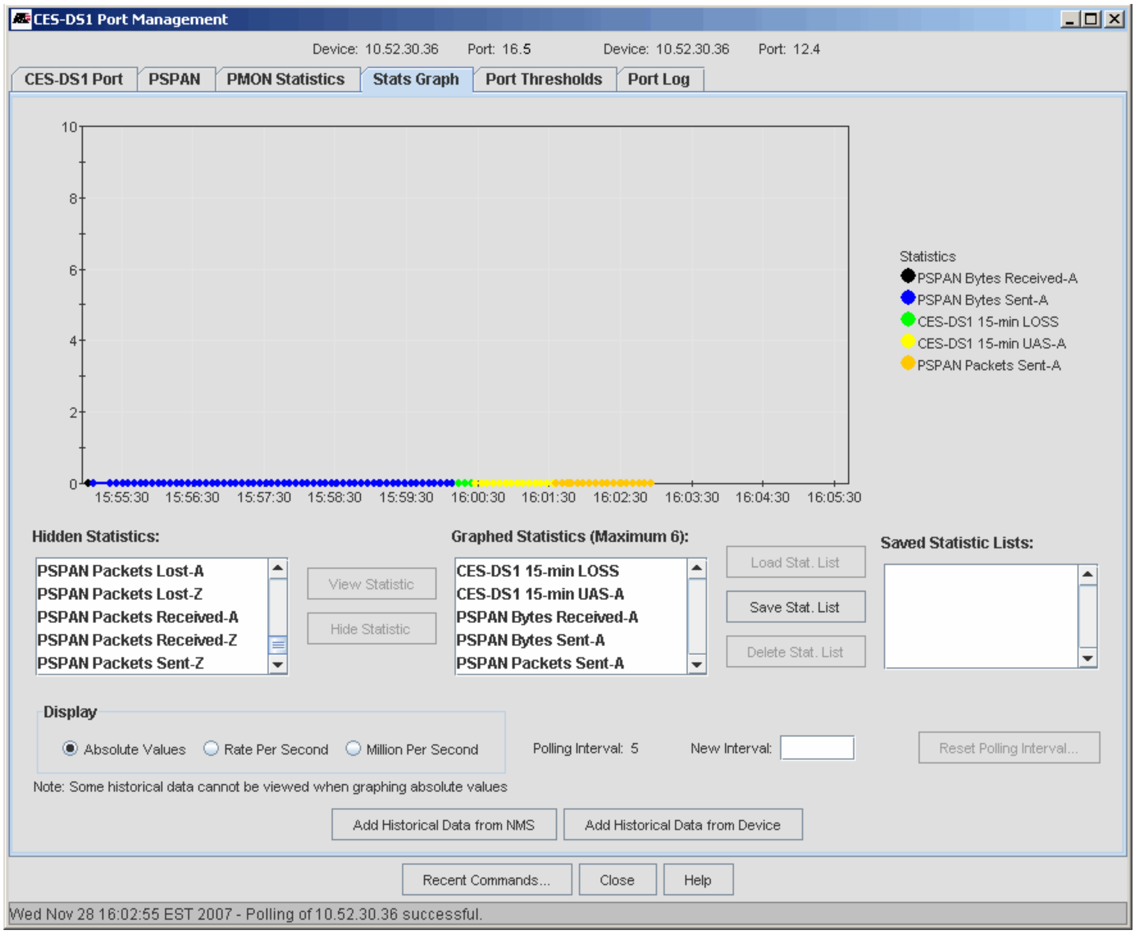
```
Wed Nov 28 15:53:13 EST 2007 - Polling of 10.52.30.36 successful.
Wed Nov 28 15:53:13 EST 2007 - Polling of 10.52.30.36 successful.
```

FIGURE 16-131 PMON Statistics Tab for two Endpoints

16.13.6.4 Stats Graph Tab

This form makes graphs of the statistics and allows the stats used to be saved as a list and reloaded later. Refer to the following figure.

Note: The statistics for each endpoint have the suffix -A or -Z to identify each one. The -A is the port on the left side of the two ports shown at the top of the form, and the -Z is the right side.



CES-DS1 Port Management

Device: 10.52.30.36 Port: 16.5 Device: 10.52.30.36 Port: 12.4

Statistics
● PSPAN Bytes Received-A
● PSPAN Bytes Sent-A
● CES-DS1 15-min LOSS
● CES-DS1 15-min UAS-A
● PSPAN Packets Sent-A

Hidden Statistics:
PSPAN Packets Lost-A
PSPAN Packets Lost-Z
PSPAN Packets Received-A
PSPAN Packets Received-Z
PSPAN Packets Sent-Z

Graphed Statistics (Maximum 6):
CES-DS1 15-min LOSS
CES-DS1 15-min UAS-A
PSPAN Bytes Received-A
PSPAN Bytes Sent-A
PSPAN Packets Sent-A

Saved Statistic Lists:

Display
● Absolute Values ○ Rate Per Second ○ Million Per Second

Polling Interval: 5 New Interval:

Note: Some historical data cannot be viewed when graphing absolute values

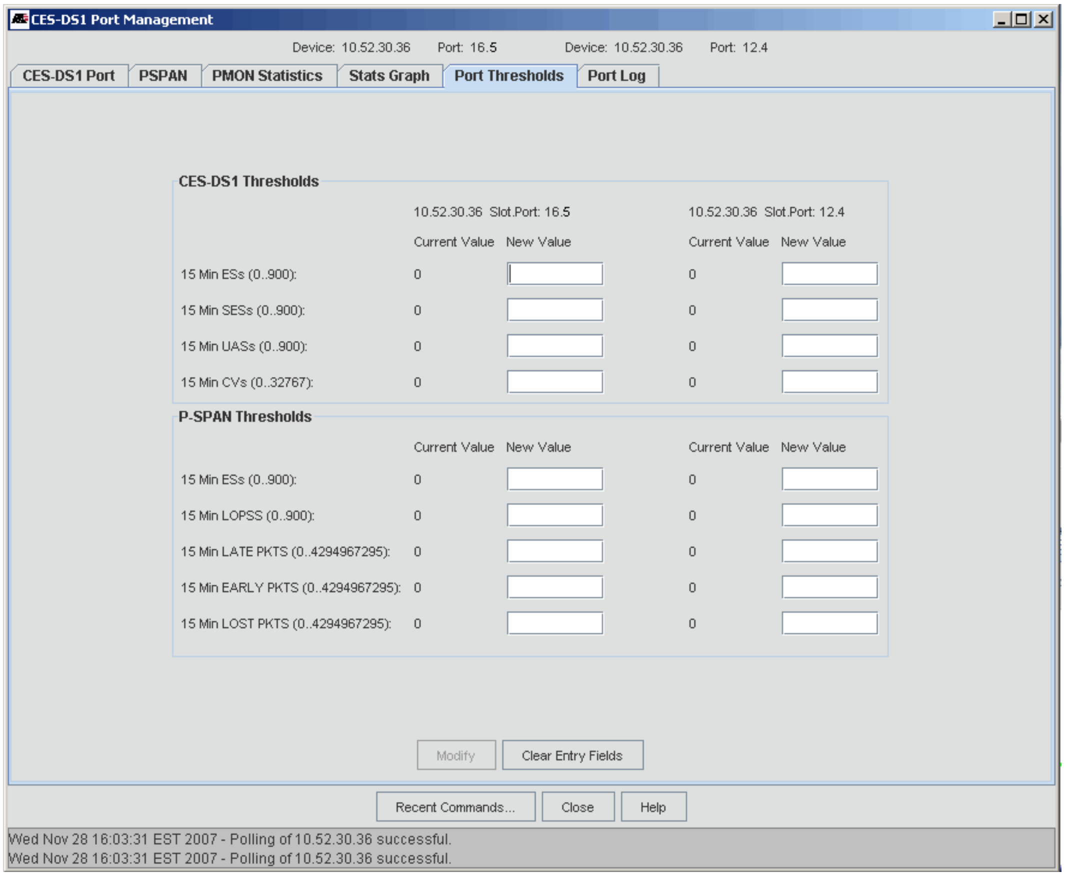
Wed Nov 28 16:02:55 EST 2007 - Polling of 10.52.30.36 successful.

FIGURE 16-132 Stats Graph Tab for two Endpoints

16.13.6.5 Port Thresholds Tab

This form allows the user to modify the threshold values for the DS1/E1 and PSPAN statisitcs.When a new value is entered in the New Value field, the Modify button is enabled.

Note: In most cases, the DS1/E1 values are not modified because they are part of the DS1/E1 port profile; if the user does change a value, the port is now out of sync with its associated profile, and an "" will appear next to the Profile name on the DS1/E1 Port tab form (as well as the Port Inventory table). In the dual endpoint configuration, the "*" will appear next to the specific port where the values were changed from the Profile. To Resync the port, the user must re-apply the profile on the DS1/E1 tab form, which puts the values back to what they are in the Profile.*



Device: 10.52.30.36 Port: 16.5 Device: 10.52.30.36 Port: 12.4

CES-DS1 Thresholds

	10.52.30.36 Slot.Port: 16.5		10.52.30.36 Slot.Port: 12.4	
	Current Value	New Value	Current Value	New Value
15 Min ESs (0..900):	0		0	
15 Min SESs (0..900):	0		0	
15 Min UASs (0..900):	0		0	
15 Min CVs (0..32767):	0		0	

P-SPAN Thresholds

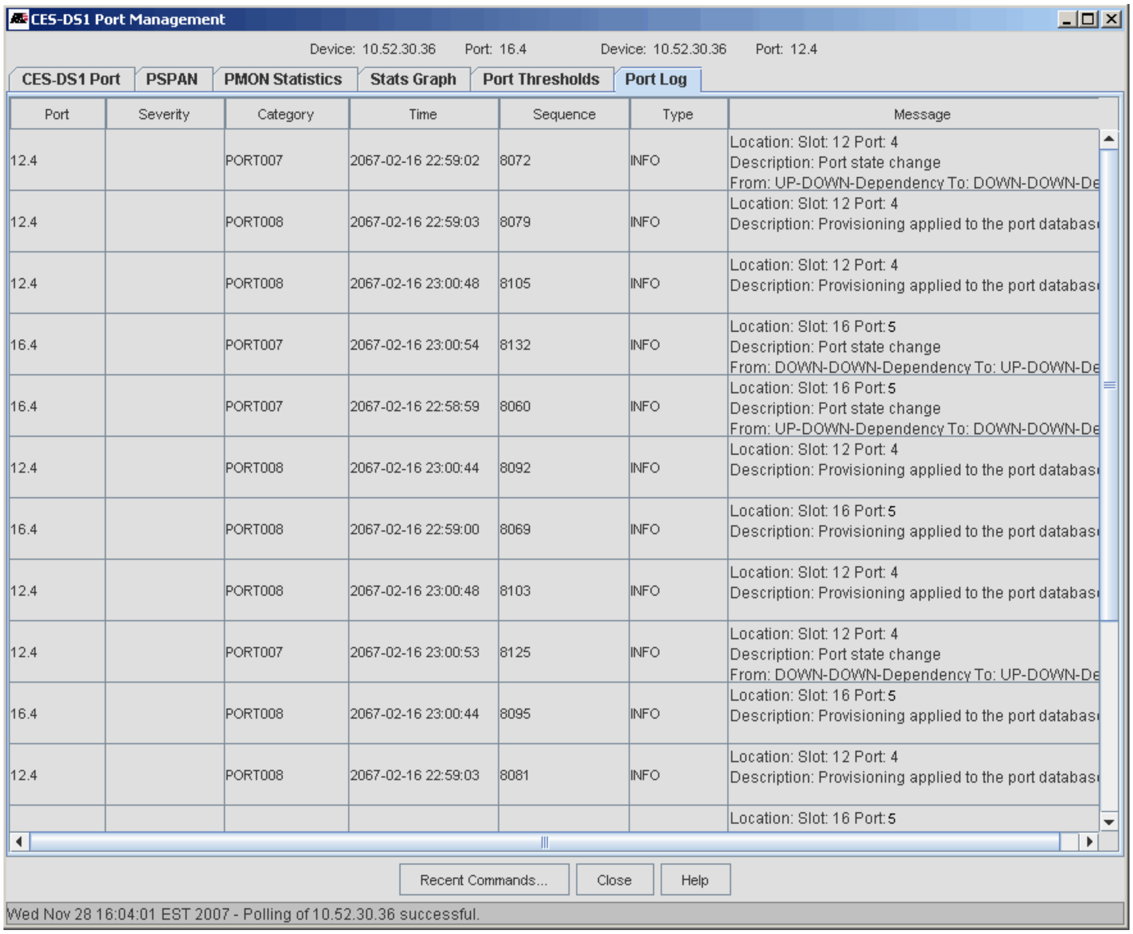
	Current Value	New Value	Current Value	New Value
15 Min ESs (0..900):	0		0	
15 Min LOPSS (0..900):	0		0	
15 Min LATE PKTS (0..4294967295):	0		0	
15 Min EARLY PKTS (0..4294967295):	0		0	
15 Min LOST PKTS (0..4294967295):	0		0	

```
Wed Nov 28 16:03:31 EST 2007 - Polling of 10.52.30.36 successful.
Wed Nov 28 16:03:31 EST 2007 - Polling of 10.52.30.36 successful.
```

FIGURE 16-133 Port Thresholds Graph Tab for two Endpoints

16.13.6.6 Port Log Tag

The following figure shows the Port Log tab for the two endpoints. Note that since these cards are on the same device; there is no need for a device column, and the Device name repeated twice on the top of the form. (If the two endpoints were on different devices, a Device column would be added, and the user could sort by Device.)



Device: 10.52.30.36 Port: 16.4 Device: 10.52.30.36 Port: 12.4

Port	Severity	Category	Time	Sequence	Type	Message
12.4		PORT007	2067-02-16 22:59:02	8072	INFO	Location: Slot: 12 Port: 4 Description: Port state change From: UP-DOWN-Dependency To: DOWN-DOWN-De
12.4		PORT008	2067-02-16 22:59:03	8079	INFO	Location: Slot: 12 Port: 4 Description: Provisioning applied to the port databas
12.4		PORT008	2067-02-16 23:00:48	8105	INFO	Location: Slot: 12 Port: 4 Description: Provisioning applied to the port databas
16.4		PORT007	2067-02-16 23:00:54	8132	INFO	Location: Slot: 16 Port:5 Description: Port state change From: DOWN-DOWN-Dependency To: UP-DOWN-De
16.4		PORT007	2067-02-16 22:58:59	8060	INFO	Location: Slot: 16 Port:5 Description: Port state change From: UP-DOWN-Dependency To: DOWN-DOWN-De
12.4		PORT008	2067-02-16 23:00:44	8092	INFO	Location: Slot: 12 Port: 4 Description: Provisioning applied to the port databas
16.4		PORT008	2067-02-16 22:59:00	8069	INFO	Location: Slot: 16 Port:5 Description: Provisioning applied to the port databas
12.4		PORT008	2067-02-16 23:00:48	8103	INFO	Location: Slot: 12 Port: 4 Description: Provisioning applied to the port databas
12.4		PORT007	2067-02-16 23:00:53	8125	INFO	Location: Slot: 12 Port: 4 Description: Port state change From: DOWN-DOWN-Dependency To: UP-DOWN-De
16.4		PORT008	2067-02-16 23:00:44	8095	INFO	Location: Slot: 16 Port:5 Description: Provisioning applied to the port databas
12.4		PORT008	2067-02-16 22:59:03	8081	INFO	Location: Slot: 12 Port: 4 Description: Provisioning applied to the port databas
						Location: Slot: 16 Port:5

Wed Nov 28 16:04:01 EST 2007 - Polling of 10.52.30.36 successful.

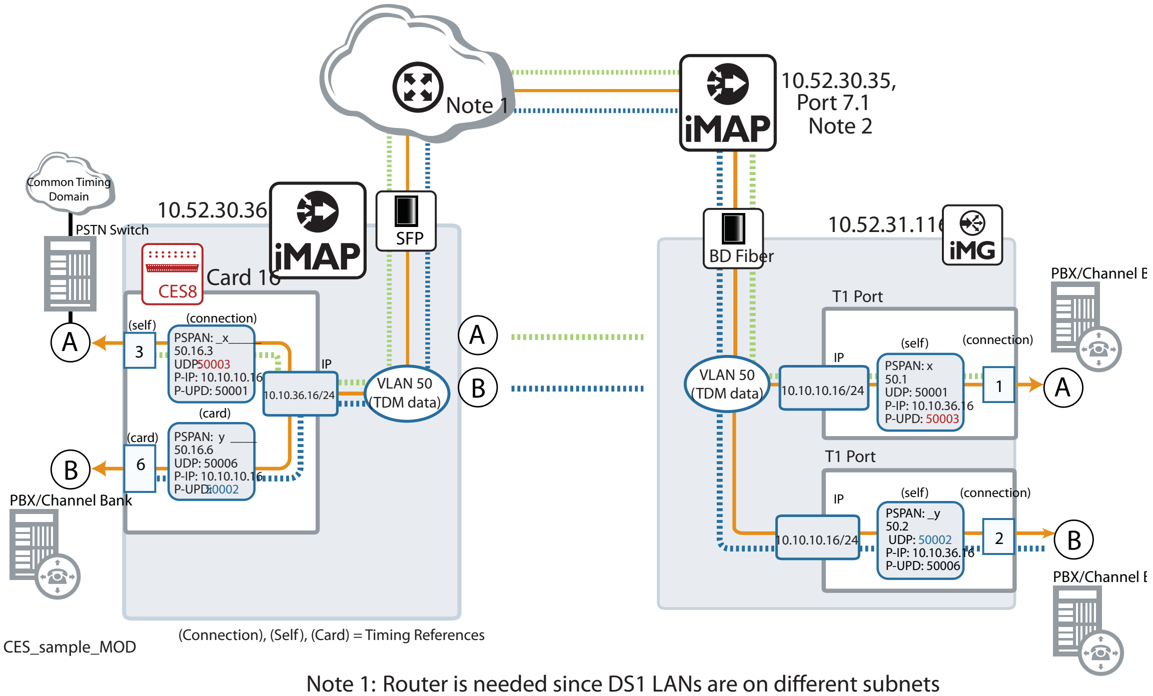
FIGURE 16-134 Port Log Tab for two Endpoints

16.13.7 Provisioning iMG6x6MOD with T1/E1 Card and CES

In release 10.0, it is possible to configure an iMG6x6MOD with a T1/E1 card. This card has two ports, where **both** are configured as either DS1 or E1 signal formats (for the two T1 or E1 ports respectively). The DS1 configuration (T1) is shown below.

At the other end of the DS1 connection, a CES8 port can be configured. Provisioning this iMG-CES8 port connection is similar to the CES8-CES8 port connection as shown in "Provision the Two DS1 Ports" on page 627, since the parameters datafilled on the iMG6x6MOD are similar to those for the CES8. However, there are some key differences in the use of profiles and the Triple-Play provisioning, in that all services, not just CES, are provisioned together on the iMG, while only the individual CES port is provisioned on the iMAP CES8 card.

First, refer to Figure 16-135, which shows how each DS1 port on the iMG can be connected with separate ports on the CES8 card. Included are the parameters that need to be datafilled at each endpoint.



Note 1: Router is needed since DS1 LANs are on different subnets
(10.10.36.0/24 and 10.10.10.0/24)

Note 2: Other iMAPs in network would provide topology (EPSR) for VLAN
(In this case, 10.52.30.35 connects over port 7.1 to iMG6x6MOD)

FIGURE 16-135 CES8 to iMG6x6MOD Connections

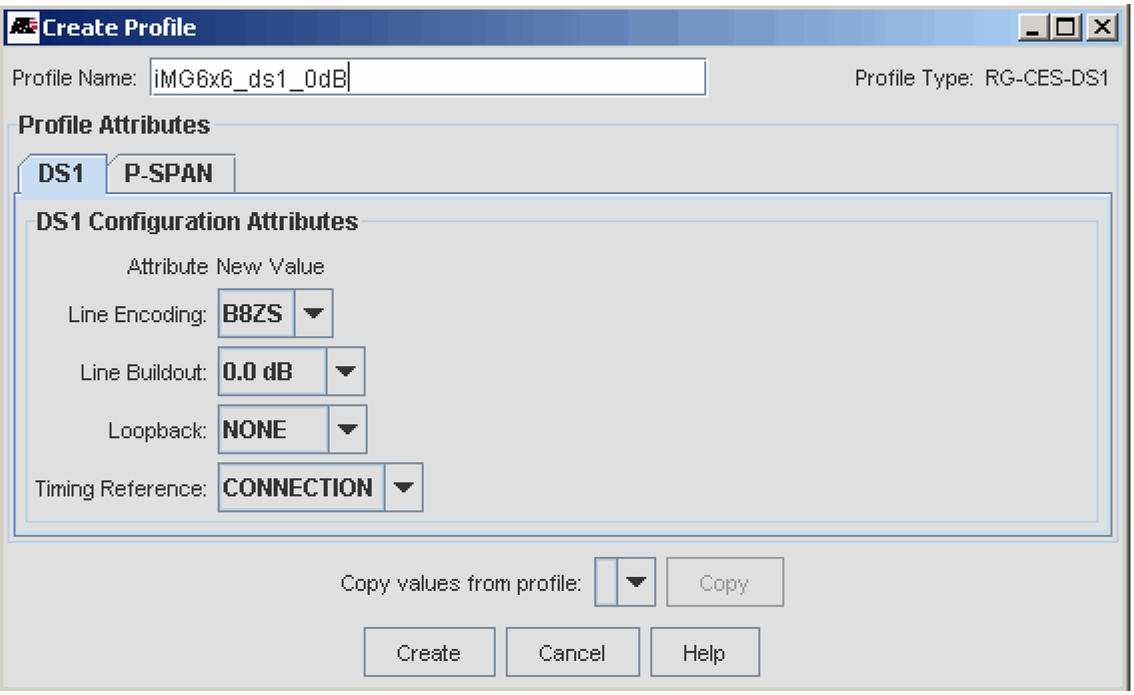
Provisioning this involves the following steps.

Note: This example assumes a DS1 connection. An E1 example would be similar.

16.13.7.1 Create RG_CES_DS1 Profiles

This has similar attributes to the iMAP CES DS1 profile, except that this will be for a DS1 port on the iMG6x6MOD. Select *Network Services -> Profile -> iMG/RG Service Profiles -> Create iMG/RG CES-DS1 Port Profile*. Refer to the following figures which show two profiles; each profile could be applied to a different DS1 port on the CES card on the iMG6x6MOD. Key attributes are:

- A Timing Reference parameter is included with values { Self | Connection | Internal } on the DS1/E1 Tab. It's value should be compatible with the Peer end. (Note that there is no CARD value for the RG..)
- Line Encoding



Profile Name: iMG6x6_ds1_0dB

Profile Type: RG-CES-DS1

Line Encoding: B8ZS

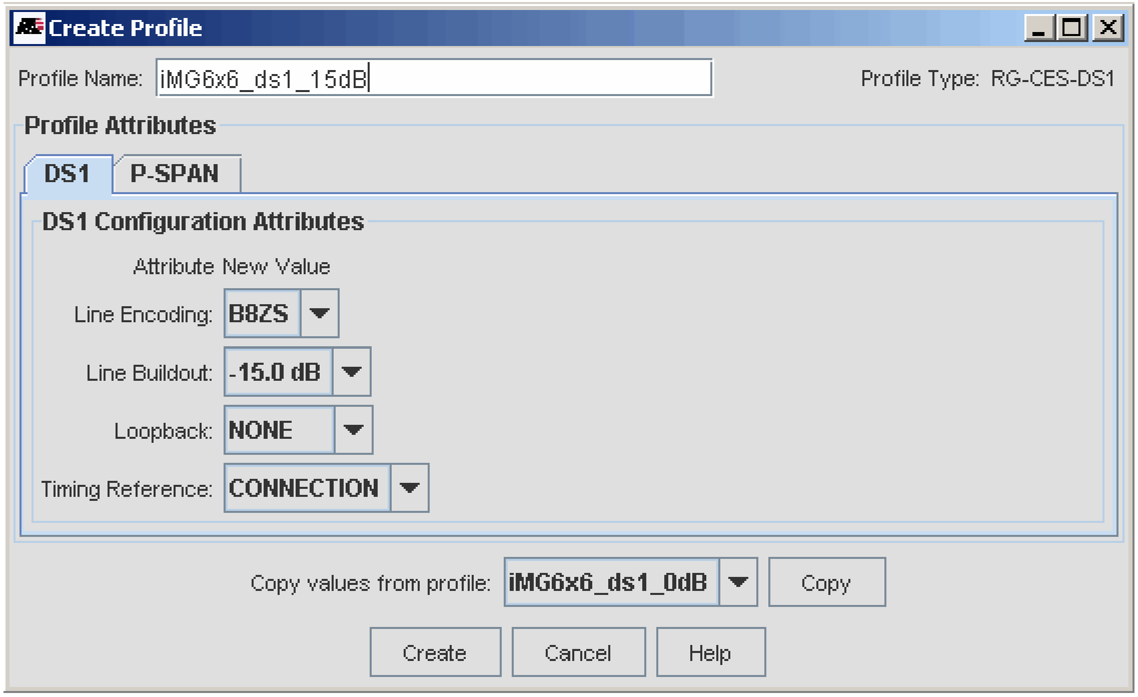
Line Buildout: 0.0 dB

Loopback: NONE

Timing Reference: CONNECTION

Copy values from profile:

FIGURE 16-136 Creating a RG-CES-DS1 Profile - DS1 (0dB)



Create Profile

Profile Name: iMG6x6_ds1_15dB

Profile Type: RG-CES-DS1

Profile Attributes

DS1 Configuration Attributes

Attribute New Value

Line Encoding: B8ZS

Line Buildout: -15.0 dB

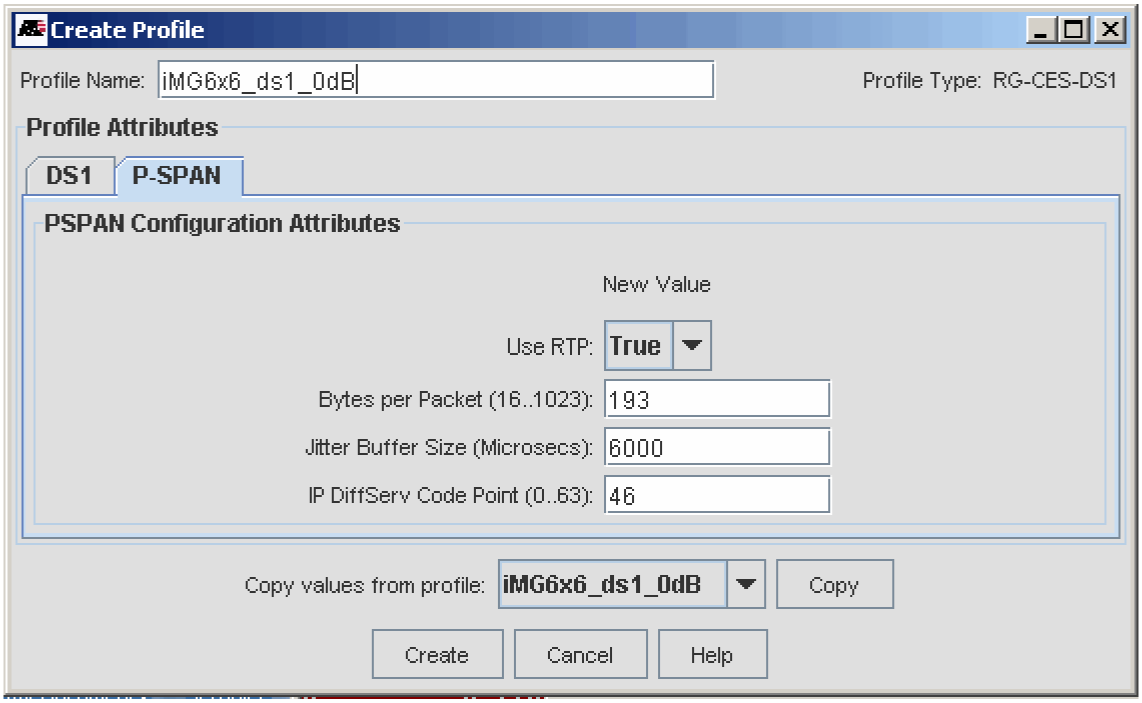
Loopback: NONE

Timing Reference: CONNECTION

Copy values from profile: iMG6x6_ds1_0dB

FIGURE 16-137 Creating a RG-CES-DS1 Profile - DS1 (15 dB)

The following figure shows the PSPAN tab attributes that are datafilled as part of the RG-CES DS profile. The key attributes RTP and Bytes per Packet should match the Peer end.



Create Profile

Profile Name: iMG6x6_ds1_0dB

Profile Type: RG-CES-DS1

Profile Attributes

PSPAN Configuration Attributes

New Value

Use RTP: True

Bytes per Packet (16..1023): 193

Jitter Buffer Size (Microsecs): 6000

IP DiffServ Code Point (0..63): 46

Copy values from profile: iMG6x6_ds1_0dB

FIGURE 16-138 Creating a RG-CES-DS1 Profile - PSPAN

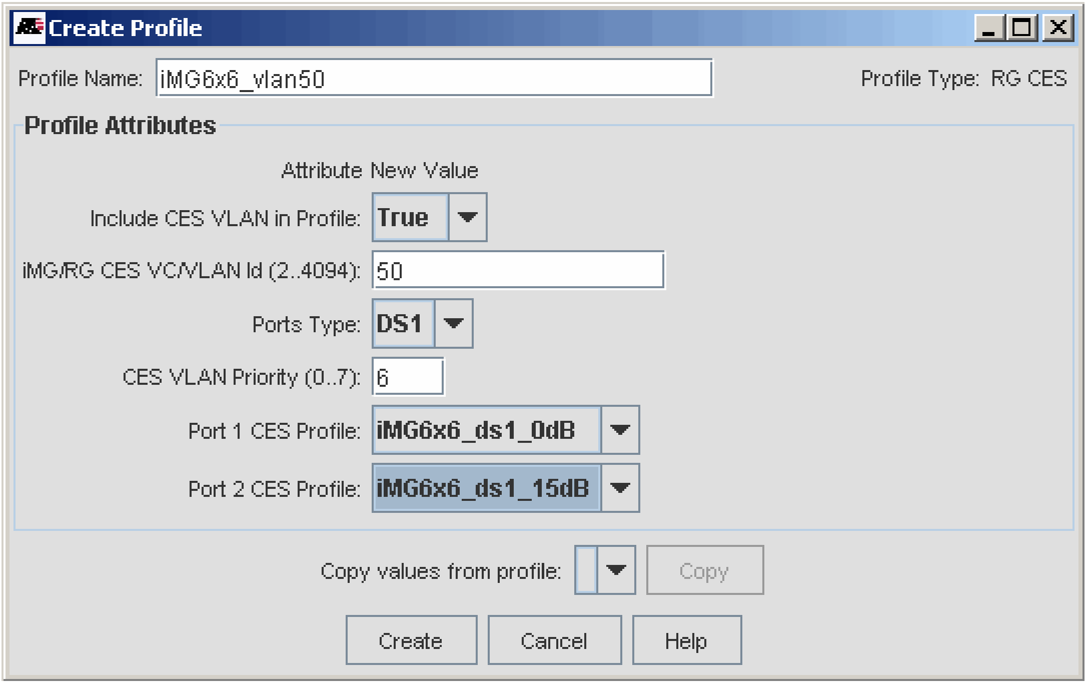
16.13.7.2 Create an iMG/RG CES Service Profile

Select *Network Services -> Profile -> Create iMG CES- Service Profile*. Refer to the following figures.

Key attributes are:

- Ports Type: {DS1/E1}
- CES VLAN ID - This is used if the Open Access model is being used. See "Create an iMG/RG General Profile" on page 640.
- Port 1 RG-CES Port Profile
- Port 2 RG-CES Port Profile

The CES VLAN ID can be specified here to support common CES VLANs across customers. The RG-CES Port Profiles will also be used in the Port Management screens when RG port details are displayed.


Create Profile

Profile Name: iMG6x6_vlan50

Profile Type: RG CES

Profile Attributes

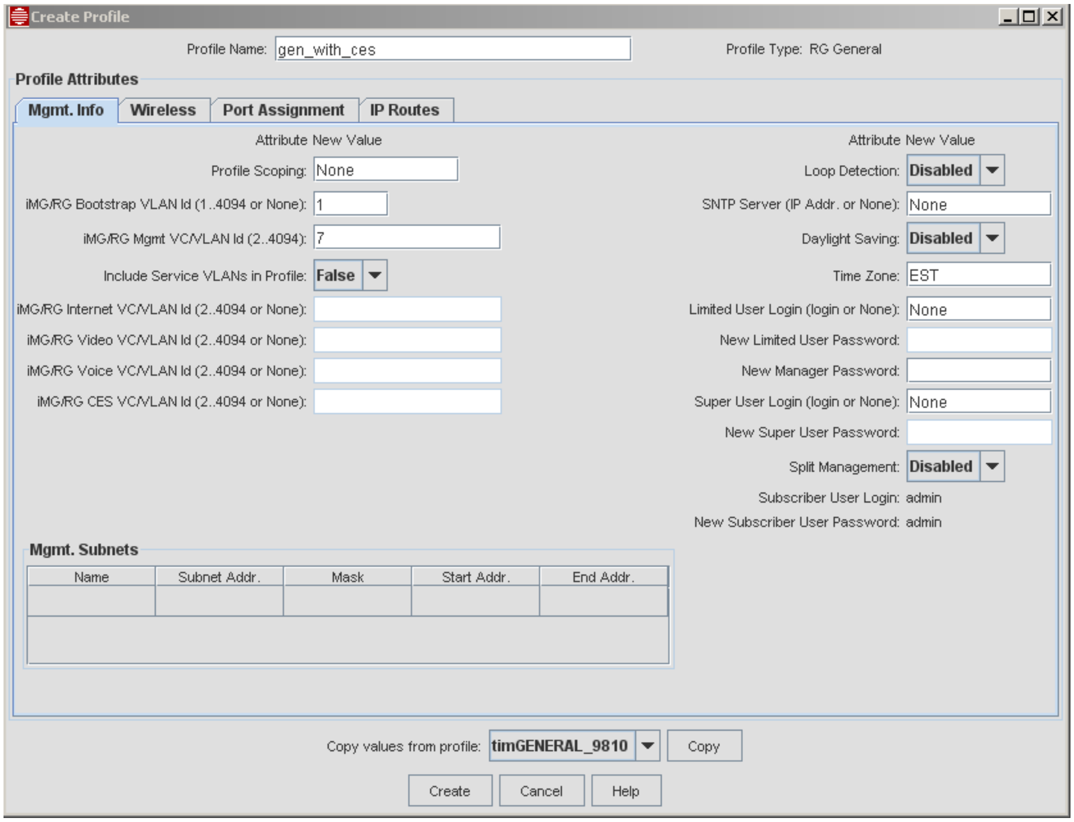
Attribute	New Value
Include CES VLAN in Profile:	True
iMG/RG CES VC/VLAN Id (2..4094):	50
Ports Type:	DS1
CES VLAN Priority (0..7):	6
Port 1 CES Profile:	iMG6x6_ds1_0dB
Port 2 CES Profile:	iMG6x6_ds1_15dB

Copy values from profile:

FIGURE 16-139 iMG CES Service Profile

16.13.7.3 Create an iMG/RG General Profile

Create an iMG/RG General Profile. This has attributes for provisioning other services on the iMG6x6MOD as well as other iMG/RG types. Note that there is a CES VLAN Id field. If the Access Island model is being used, set the Include Service VLAN in Profile to True, and the VLANs are editable. For Open Access, set this to False, so that VLANs are filled in for the iMG/RG Profiles for each service type. (In this example, it would be set to False, since for the RG CES Profile the Include option was set to True with a VLAN ID of 50. Refer to the following figure.



Profile Name: gen_with_ces

Profile Type: RG General

Profile Scoping: None

iMG/RG Bootstrap VLAN Id (1..4094 or None): 1

iMG/RG Mgmt VC/VLAN Id (2..4094): 7

Include Service VLANs in Profile: False

iMG/RG Internet VC/VLAN Id (2..4094 or None):

iMG/RG Video VC/VLAN Id (2..4094 or None):

iMG/RG Voice VC/VLAN Id (2..4094 or None):

iMG/RG CES VC/VLAN Id (2..4094 or None):

Loop Detection: Disabled

SNTP Server (IP Addr. or None): None

Daylight Saving: Disabled

Time Zone: EST

Limited User Login (login or None): None

New Limited User Password:

New Manager Password:

Super User Login (login or None): None

New Super User Password:

Split Management: Disabled

Subscriber User Login: admin

New Subscriber User Password: admin

Mgmt. Subnets

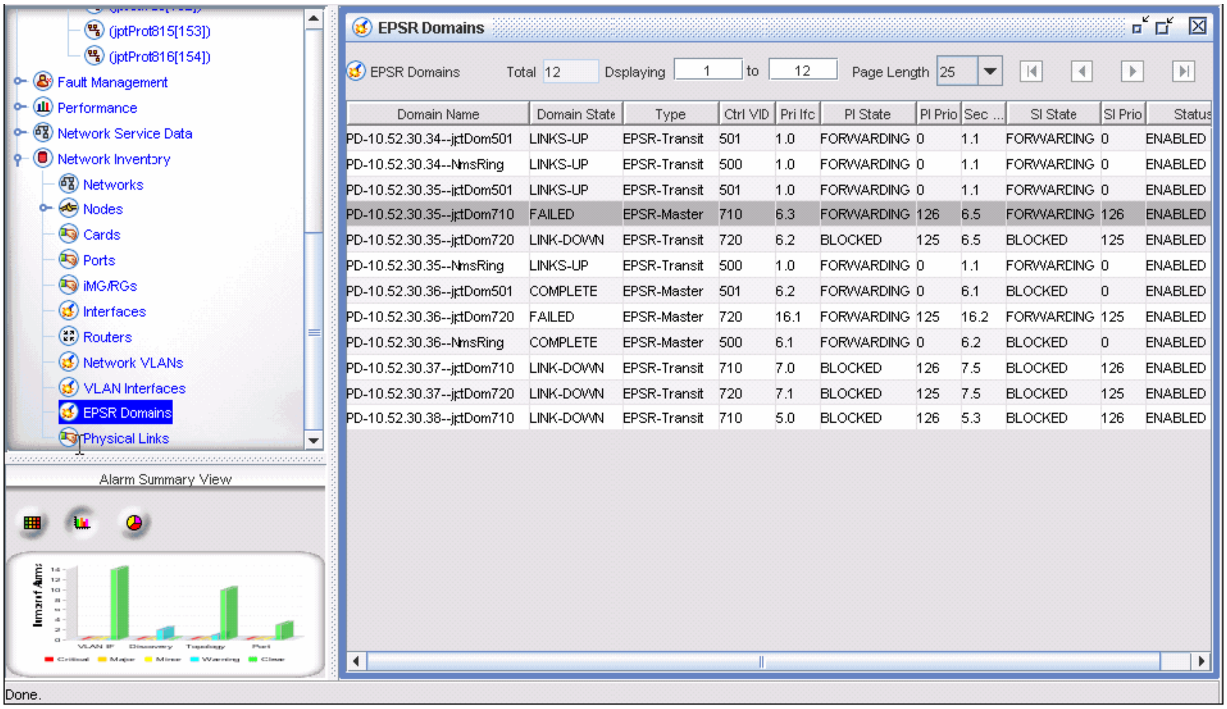
Name	Subnet Addr.	Mask	Start Addr.	End Addr.

Copy values from profile: timGENERAL_9810

FIGURE 16-140 iMG/RG General Profile - includes CES DS1 VLAN

16.13.7.4 Provision the Triple-Play Form

There are different strategies to provisioning the iMG/RG. In this example, the iMG646MOD is already known to the iMAP, and now the Triple Play Form will be filled out and then applied. Refer to the following figure.

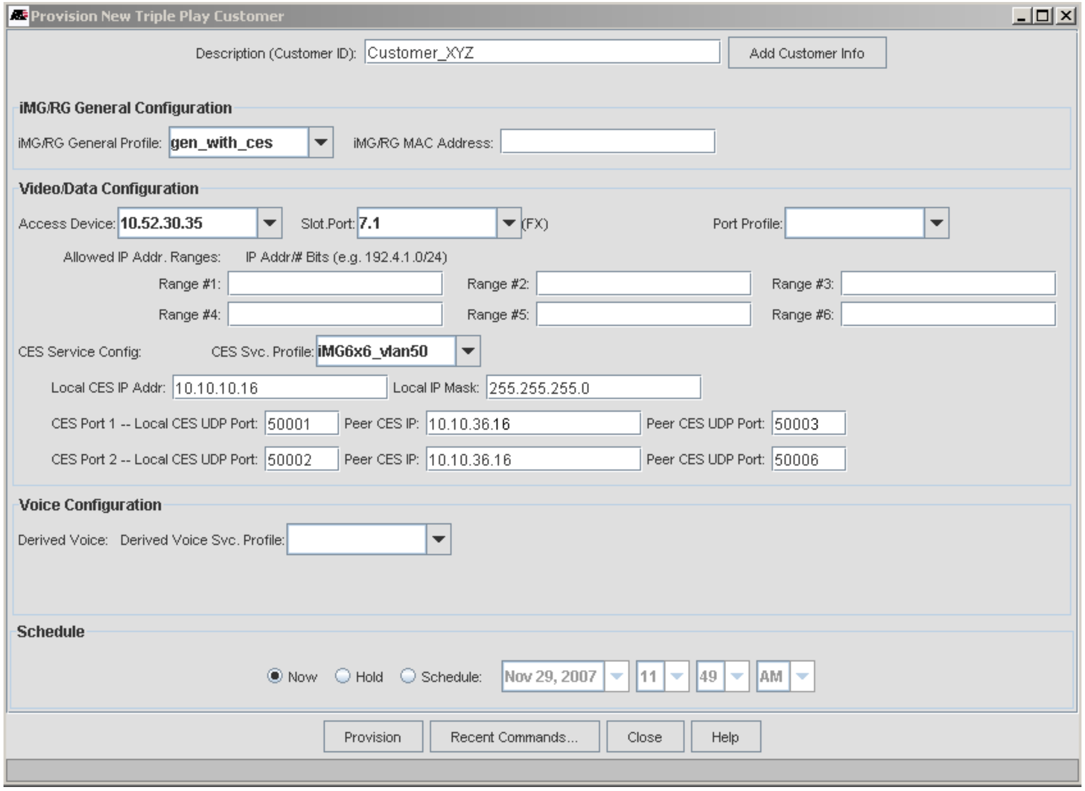


EPSR Domains Total 12 Dsplaying 1 to 12 Page Length 25

Domain Name	Domain State	Type	Ctrl VID	Pri Ifc	PI State	PI Prio	Sec ...	SI State	SI Prio	Status
PD-10.52.30.34--jctDom501	LINKS-UP	EPSR-Transit	501	1.0	FORWARDING	0	1.1	FORWARDING	0	ENABLED
PD-10.52.30.34--NmsRing	LINKS-UP	EPSR-Transit	500	1.0	FORWARDING	0	1.1	FORWARDING	0	ENABLED
PD-10.52.30.35--jctDom501	LINKS-UP	EPSR-Transit	501	1.0	FORWARDING	0	1.1	FORWARDING	0	ENABLED
PD-10.52.30.35--jctDom710	FAILED	EPSR-Master	710	6.3	FORWARDING	126	6.5	FORWARDING	126	ENABLED
PD-10.52.30.35--jctDom720	LINK-DOWN	EPSR-Transit	720	6.2	BLOCKED	125	6.5	BLOCKED	125	ENABLED
PD-10.52.30.35--NmsRing	LINKS-UP	EPSR-Transit	500	1.0	FORWARDING	0	1.1	FORWARDING	0	ENABLED
PD-10.52.30.36--jctDom501	COMPLETE	EPSR-Master	501	6.2	FORWARDING	0	6.1	BLOCKED	0	ENABLED
PD-10.52.30.36--jctDom720	FAILED	EPSR-Master	720	16.1	FORWARDING	125	16.2	FORWARDING	125	ENABLED
PD-10.52.30.36--NmsRing	COMPLETE	EPSR-Master	500	6.1	FORWARDING	0	6.2	BLOCKED	0	ENABLED
PD-10.52.30.37--jctDom710	LINK-DOWN	EPSR-Transit	710	7.0	BLOCKED	126	7.5	BLOCKED	126	ENABLED
PD-10.52.30.37--jctDom720	LINK-DOWN	EPSR-Transit	720	7.1	BLOCKED	125	7.5	BLOCKED	125	ENABLED
PD-10.52.30.38--jctDom710	LINK-DOWN	EPSR-Transit	710	5.0	BLOCKED	126	5.3	BLOCKED	126	ENABLED

FIGURE 16-141 Provisioning the iMG646MOD for Triple Play Service

In the Triple Play form that comes up, this screen will allow the user to select an iMG/RG General Profile in which a new CES Service Configuration section will appear. Refer to the following figure.



Provision New Triple Play Customer

Description (Customer ID): Customer_XYZ

iMG/RG General Configuration

iMG/RG General Profile: gen_with_ces

iMG/RG MAC Address:

Video/Data Configuration

Access Device: 10.52.30.35

Slot.Port: 7.1 (FX)

Port Profile:

Allowed IP Addr. Ranges: IP Addr/# Bits (e.g. 192.4.1.0/24)

Range #1: Range #2: Range #3:

Range #4: Range #5: Range #6:

CES Service Config: CES Svc. Profile: iMG6x6_vlan50

Local CES IP Addr: 10.10.10.16 Local IP Mask: 255.255.255.0

CES Port 1 -- Local CES UDP Port: 50001 Peer CES IP: 10.10.36.16 Peer CES UDP Port: 50003

CES Port 2 -- Local CES UDP Port: 50002 Peer CES IP: 10.10.36.16 Peer CES UDP Port: 50006

Voice Configuration

Derived Voice: Derived Voice Svc. Profile:

Schedule

● Now ○ Hold ○ Schedule: Nov 29, 2007 11 49 AM

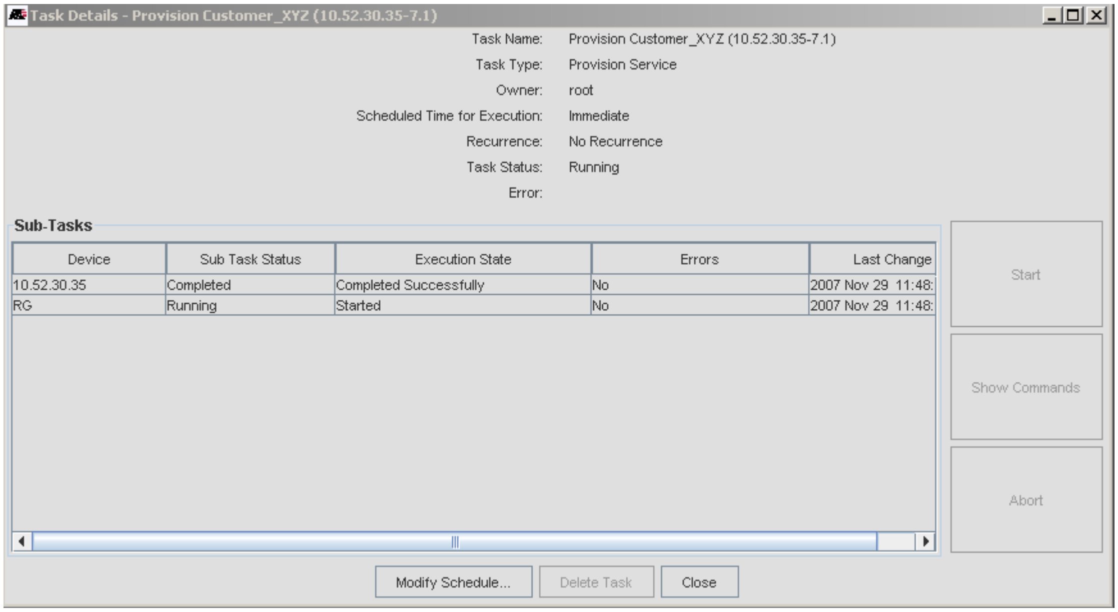
FIGURE 16-142 Triple Play Form - Selecting General Profile brings up CES Service Config

Selection of the CES Service Profile permits entry of the following parameters.

- CES Service Profile (an RG CES Service Profile - for required module and port attributes)
- Local CES IP and mask (for the CES module being provisioned - Module specific)
- CES Port 1: will need LocalUDP, PeerIP, and PeerUDP (customer specific)
- CES Port 2: will need LocalUDP, PeerIP, and PeerUDP (customer specific)

The Provision Button becomes active after specifying the required parameters and the CustomerID (at the top).

The provision tasks are run when the Provision Button is pressed. Refer to the following figure.When finished, the user has the option of Provisioning a new subscriber.



Task Name: Provision Customer_XYZ (10.52.30.35-7.1)
Task Type: Provision Service
Owner: root
Scheduled Time for Execution: Immediate
Recurrence: No Recurrence
Task Status: Running
Error:

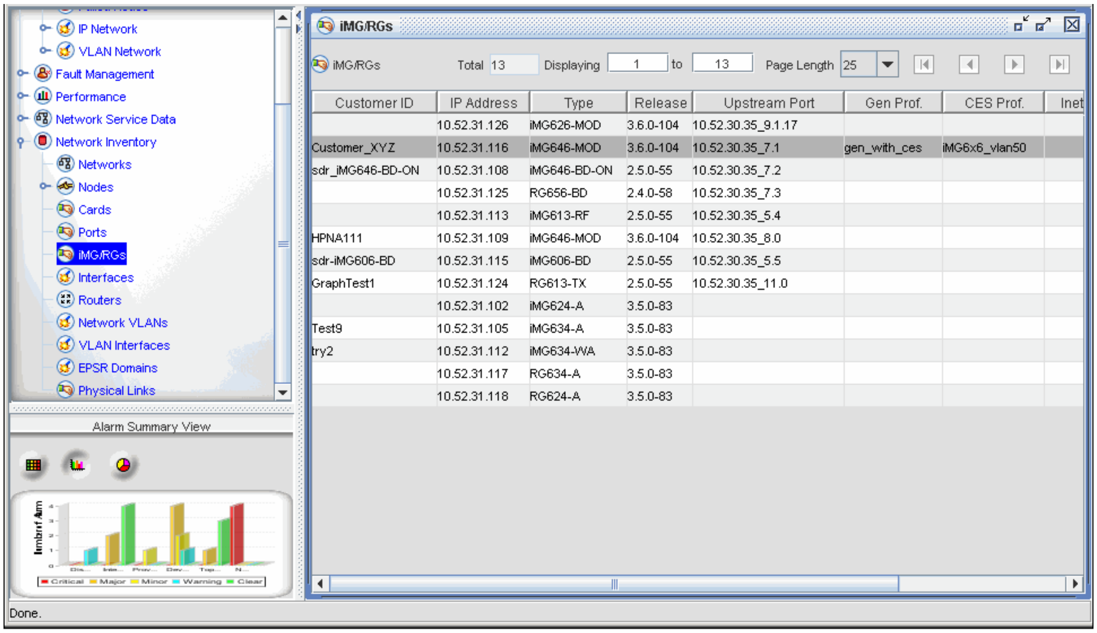
Sub-Tasks

Device	Sub Task Status	Execution State	Errors	Last Change
10.52.30.35	Completed	Completed Successfully	No	2007 Nov 29 11:48:
RG	Running	Started	No	2007 Nov 29 11:48:

FIGURE 16-143 Task Panel as iMG646MOD/T1Conpletes

16.13.7.5 Viewing Results

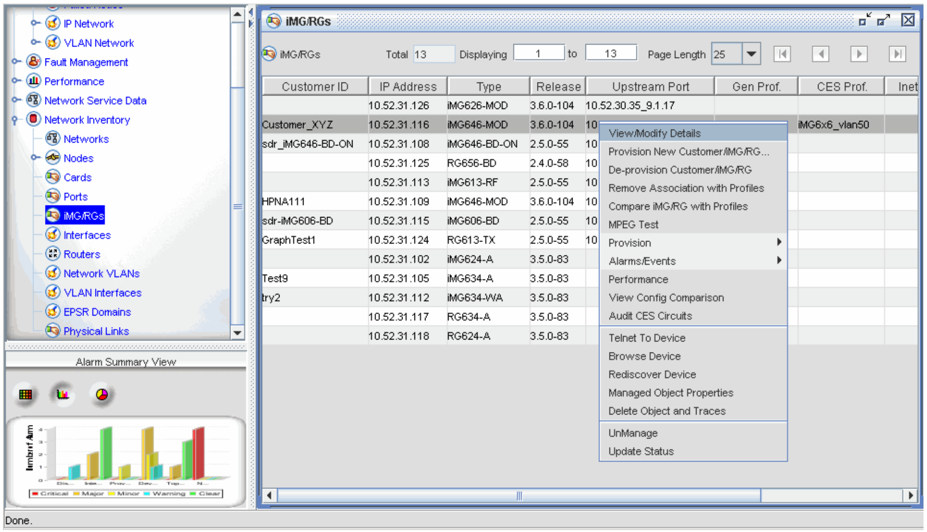
Once the iMG646MOD is provisioned, the user can view the details by going to the RG table and selecting View/Modify Details from the pull-down, as shown in the following figures.



iMG/RGs Total 13 Displaying 1 to 13 Page Length 25

Customer ID	IP Address	Type	Release	Upstream Port	Gen Prof.	CES Prof.	Inet
	10.52.31.126	iMG626-MOD	3.6.0-104	10.52.30.35_9.1.17			
Customer_XYZ	10.52.31.116	iMG646-MOD	3.6.0-104	10.52.30.35_7.1	gen_with_ces	iMG6x6_vlan50	
sdr_iMG646-BD-ON	10.52.31.108	iMG646-BD-ON	2.5.0-55	10.52.30.35_7.2			
	10.52.31.125	RG656-BD	2.4.0-58	10.52.30.35_7.3			
	10.52.31.113	iMG613-RF	2.5.0-55	10.52.30.35_5.4			
HPNA111	10.52.31.109	iMG646-MOD	3.6.0-104	10.52.30.35_8.0			
sdr-iMG606-BD	10.52.31.115	iMG606-BD	2.5.0-55	10.52.30.35_5.5			
GraphTest1	10.52.31.124	RG613-TX	2.5.0-55	10.52.30.35_11.0			
	10.52.31.102	iMG624-A	3.5.0-83				
Test9	10.52.31.105	iMG634-A	3.5.0-83				
try2	10.52.31.112	iMG634-WA	3.5.0-83				
	10.52.31.117	RG634-A	3.5.0-83				
	10.52.31.118	RG624-A	3.5.0-83				

FIGURE 16-144 iMG/RG Inventory Table with Provisioned iMG646MOD and CES Service

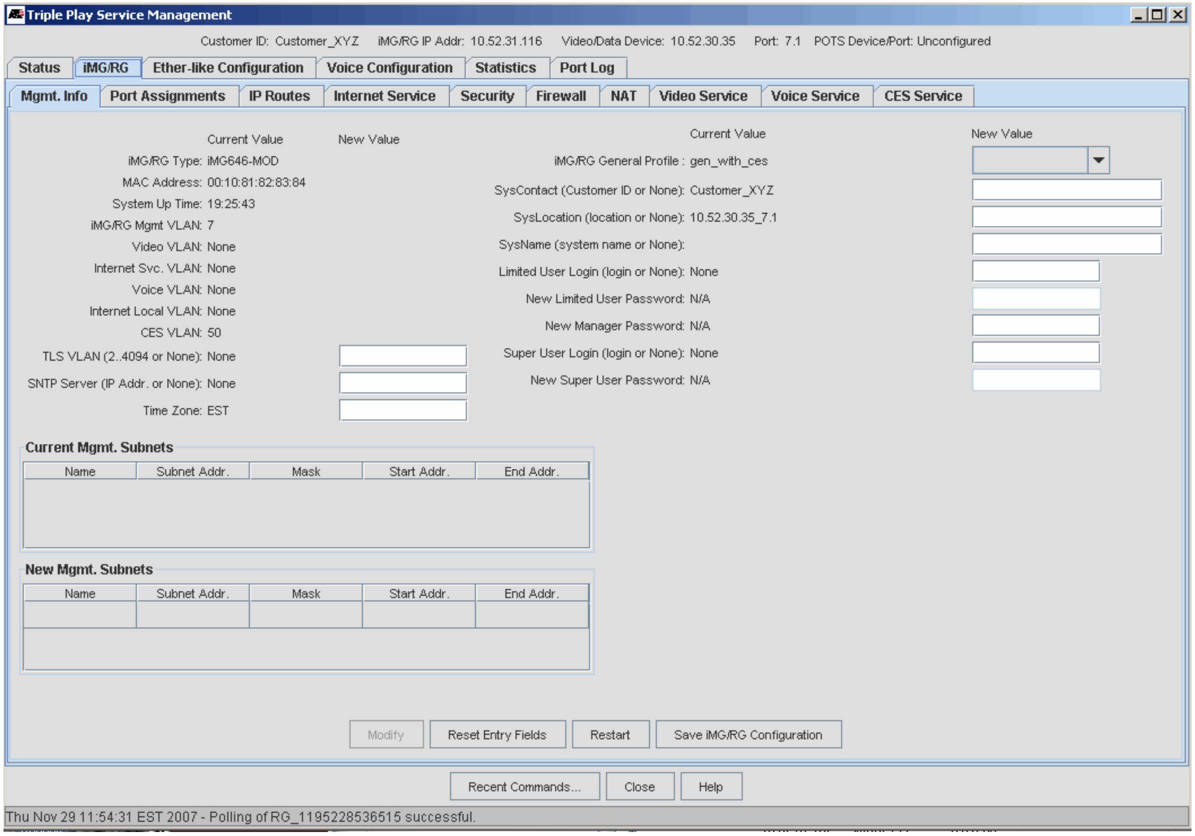


iMG/RGs Total 13 Displaying 1 to 13 Page Length 25

Customer ID	IP Address	Type	Release	Upstream Port	Gen Prof.	CES Prof.	Inet
	10.52.31.126	iMG626-MOD	3.6.0-104	10.52.30.35_9.1.17			
Customer_XYZ	10.52.31.116	iMG646-MOD	3.6.0-104	10		iMG6x6_vlan50	
sdr_iMG646-BD-ON	10.52.31.108	iMG646-BD-ON	2.5.0-55	10			
	10.52.31.125	RG656-BD	2.4.0-58	10			
	10.52.31.113	iMG613-RF	2.5.0-55	10			
HPNA111	10.52.31.109	iMG646-MOD	3.6.0-104	10			
sdr-iMG606-BD	10.52.31.115	iMG606-BD	2.5.0-55	10			
GraphTest1	10.52.31.124	RG613-TX	2.5.0-55	10			
	10.52.31.102	iMG624-A	3.5.0-83				
Test9	10.52.31.105	iMG634-A	3.5.0-83				
try2	10.52.31.112	iMG634-WA	3.5.0-83				
	10.52.31.117	RG634-A	3.5.0-83				
	10.52.31.118	RG624-A	3.5.0-83				

FIGURE 16-145 Right Clicking on the iMG646MOD and View/Modify Details

The *IMG/RG -> Mgmt Info* tab now shows the CES VLAN, similar to the other services.



Customer ID: Customer_XYZ iMG/RG IP Addr: 10.52.31.116 Video/Data Device: 10.52.30.35 Port: 7.1 POTS Device/Port: Unconfigured

	Current Value	New Value
iMG/RG Type:	iMG646-MOD	
MAC Address:	00:10:81:82:83:84	
System Up Time:	19:25:43	
iMG/RG Mgmt VLAN:	7	
Video VLAN:	None	
Internet Svc. VLAN:	None	
Voice VLAN:	None	
Internet Local VLAN:	None	
CES VLAN:	50	
TLS VLAN (2..4094 or None):	None	
SNTP Server (IP Addr. or None):	None	
Time Zone:	EST	

	Current Value	New Value
iMG/RG General Profile :	gen_with_ces	
SysContact (Customer ID or None):	Customer_XYZ	
SysLocation (location or None):	10.52.30.35_7.1	
SysName (system name or None):		
Limited User Login (login or None):	None	
New Limited User Password:	N/A	
New Manager Password:	N/A	
Super User Login (login or None):	None	
New Super User Password:	N/A	

Current Mgmt. Subnets

Name	Subnet Addr.	Mask	Start Addr.	End Addr.

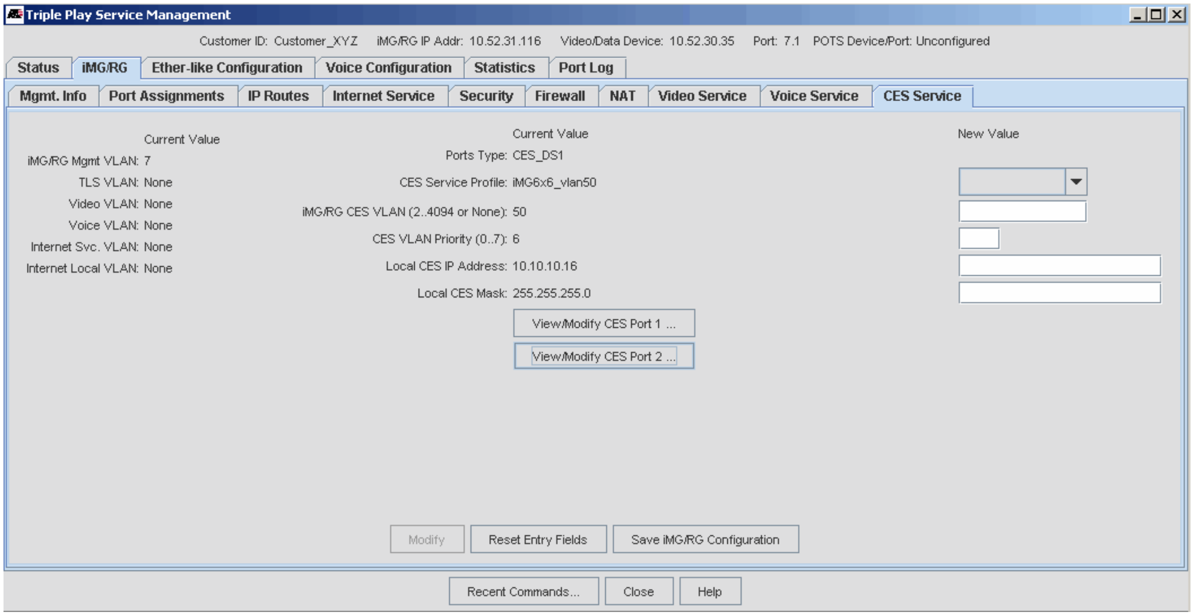
New Mgmt. Subnets

Name	Subnet Addr.	Mask	Start Addr.	End Addr.

Thu Nov 29 11:54:31 EST 2007 - Polling of RG_1195228536515 successful.

FIGURE 16-146 iMG/RG -> Mgmt Info tab

The CES Service Tab provides the specific CES parameters and allows the user to view/change the DS1 ports. Refer to the following figure



Customer ID: Customer_XYZ iMG/RG IP Addr: 10.52.31.116 Video/Data Device: 10.52.30.35 Port: 7.1 POTS Device/Port: Unconfigured

Current Value

iMG/RG Mgmt VLAN: 7
TLS VLAN: None
Video VLAN: None
Voice VLAN: None
Internet Svc. VLAN: None
Internet Local VLAN: None

Current Value

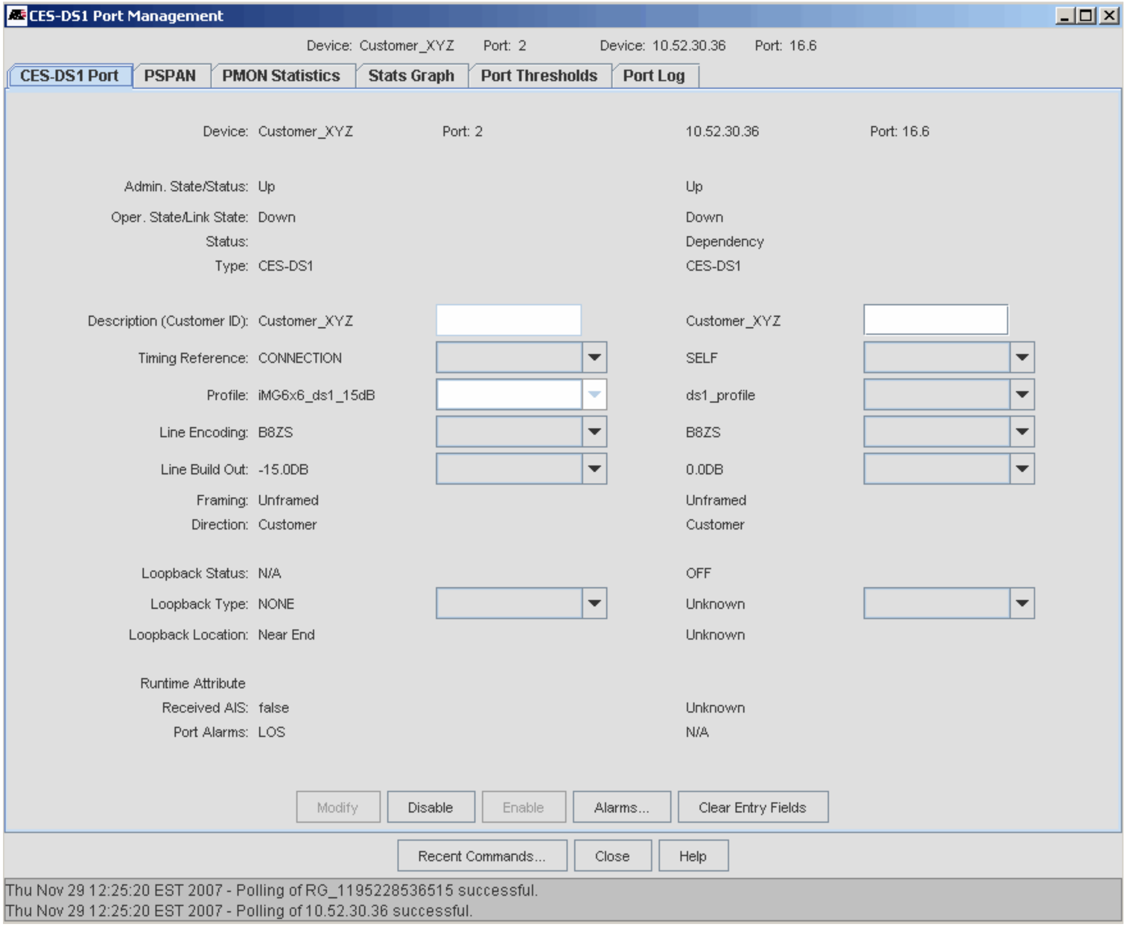
Ports Type: CES_DS1
CES Service Profile: iMG6x6_vlan50
iMG/RG CES VLAN (2..4094 or None): 50
CES VLAN Priority (0..7): 6
Local CES IP Address: 10.10.10.16
Local CES Mask: 255.255.255.0

New Value

FIGURE 16-147 View the CES Service Parameters

Selecting the View/Modify CES Port buttons brings up the CES DS1/E1 Port Management Panel, with a different panel for each port, 1 and 2. These tabs allow the user to view and change the parameters if necessary. Refer to the following figures.

Caution: Changing these parameters must be done with care, since there may be complementary parameters at the other end of the connection, and so a change in a parameter value may affect service.

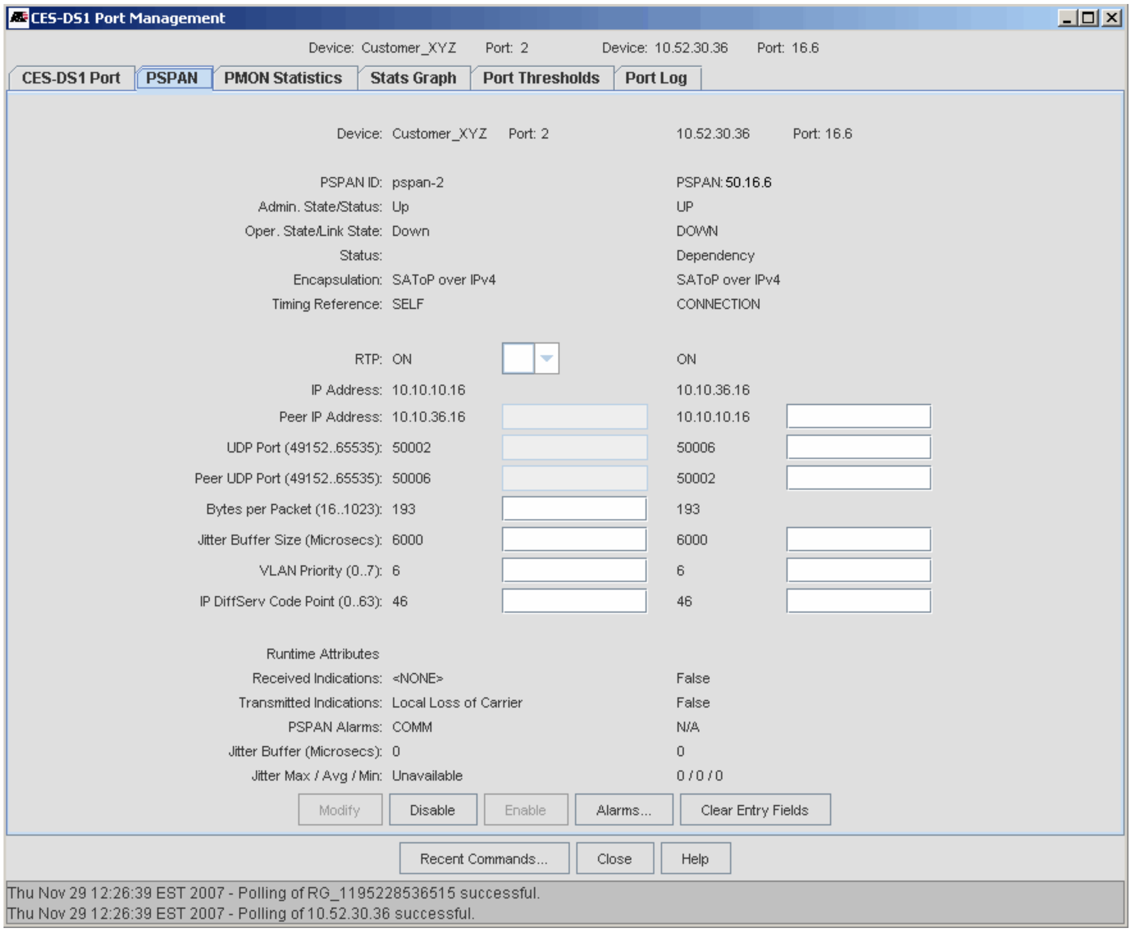


Device: Customer_XYZ Port: 2 Device: 10.52.30.36 Port: 16.6

Device:	Customer_XYZ	Port: 2	10.52.30.36	Port: 16.6
Admin. State/Status:	Up		Up	
Oper. State/Link State:	Down		Down	
Status:			Dependency	
Type:	CES-DS1		CES-DS1	
Description (Customer ID):	Customer_XYZ		Customer_XYZ	
Timing Reference:	CONNECTION		SELF	
Profile:	iMG6x6_ds1_15dB		ds1_profile	
Line Encoding:	B8ZS		B8ZS	
Line Build Out:	-15.0DB		0.0DB	
Framing:	Unframed		Unframed	
Direction:	Customer		Customer	
Loopback Status:	N/A		OFF	
Loopback Type:	NONE		Unknown	
Loopback Location:	Near End		Unknown	
Runtime Attribute				
Received AIS:	false		Unknown	
Port Alarms:	LOS		N/A	

Thu Nov 29 12:25:20 EST 2007 - Polling of RG_1195228536515 successful.
Thu Nov 29 12:25:20 EST 2007 - Polling of 10.52.30.36 successful.

FIGURE 16-148 CES-DS1 Port Parameter Form - Port 2 on the iMG6x6MOD



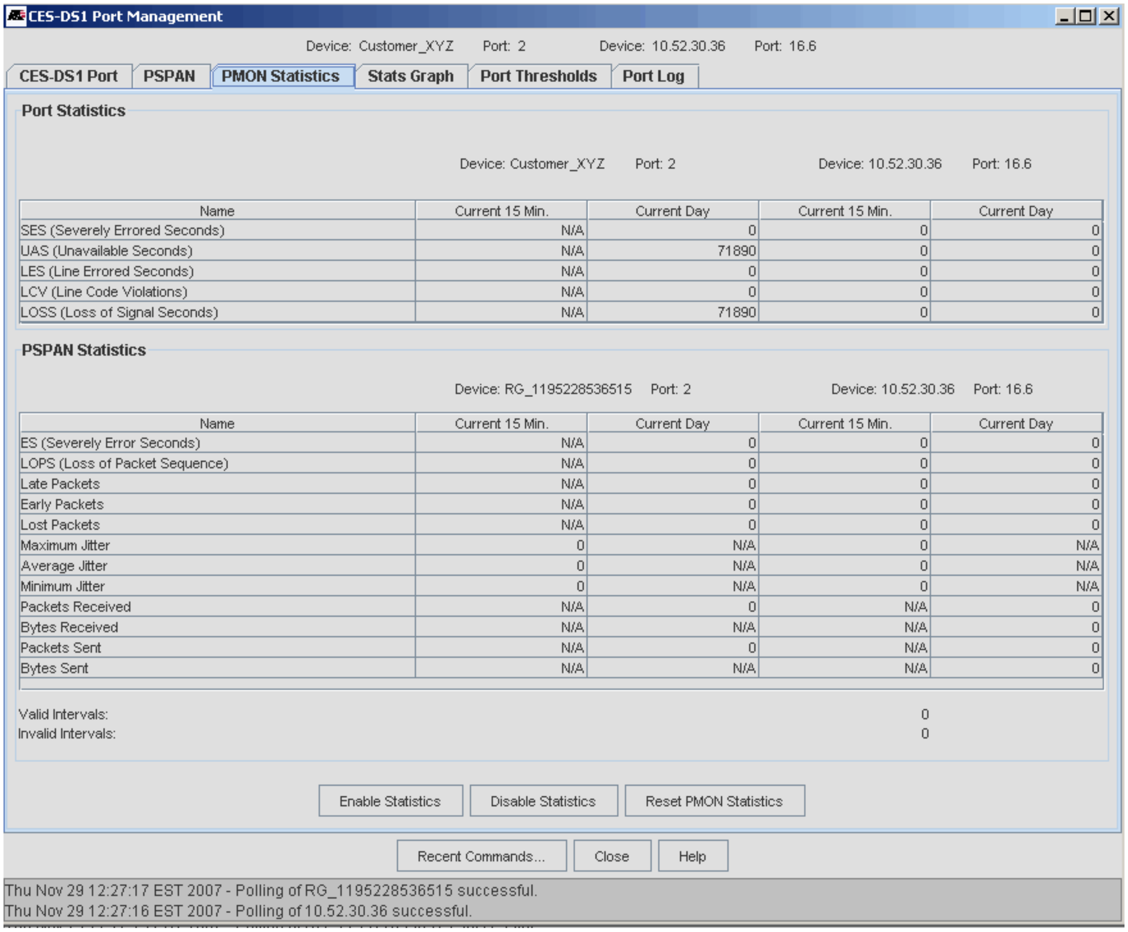
CES-DS1 Port Management

Device: Customer_XYZ Port: 2 Device: 10.52.30.36 Port: 16.6

Device:	Customer_XYZ Port: 2	10.52.30.36 Port: 16.6
PSPAN ID:	pspan-2	PSPAN:50.16.6
Admin. State/Status:	Up	UP
Oper. State/Link State:	Down	DOWN
Status:		Dependency
Encapsulation:	SAToP over IPv4	SAToP over IPv4
Timing Reference:	SELF	CONNECTION
RTP:	ON	ON
IP Address:	10.10.10.16	10.10.36.16
Peer IP Address:	10.10.36.16	10.10.10.16
UDP Port (49152..65535):	50002	50006
Peer UDP Port (49152..65535):	50006	50002
Bytes per Packet (16..1023):	193	193
Jitter Buffer Size (Microsecs):	6000	6000
VLAN Priority (0..7):	6	6
IP DiffServ Code Point (0..63):	46	46
Runtime Attributes		
Received Indications:	<NONE>	False
Transmitted Indications:	Local Loss of Carrier	False
PSPAN Alarms:	COMM	N/A
Jitter Buffer (Microsecs):	0	0
Jitter Max / Avg / Min:	Unavailable	0 / 0 / 0

```
Thu Nov 29 12:26:39 EST 2007 - Polling of RG_1195228536515 successful.
Thu Nov 29 12:26:39 EST 2007 - Polling of 10.52.30.36 successful.
```

FIGURE 16-149 CES-DS1 PSPAN Parameter Form - Port 2 on the iMG6x6MOD



Device: Customer_XYZ Port: 2 Device: 10.52.30.36 Port: 16.6

Port Statistics

Device: Customer_XYZ Port: 2 Device: 10.52.30.36 Port: 16.6

Name	Current 15 Min.	Current Day	Current 15 Min.	Current Day
SES (Severely Errored Seconds)	N/A	0	0	0
UAS (Unavailable Seconds)	N/A	71890	0	0
LES (Line Errored Seconds)	N/A	0	0	0
LCV (Line Code Violations)	N/A	0	0	0
LOSS (Loss of Signal Seconds)	N/A	71890	0	0

PSPAN Statistics

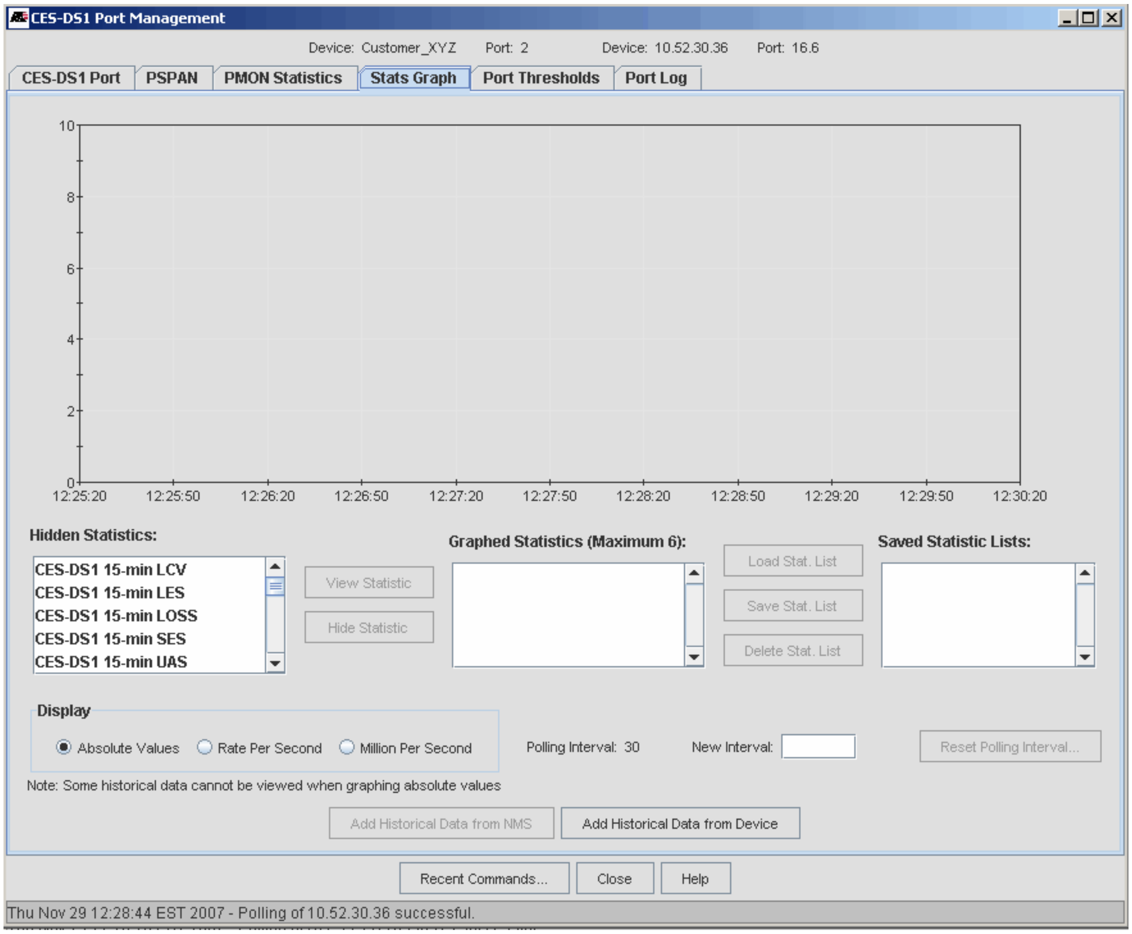
Device: RG_1195228536515 Port: 2 Device: 10.52.30.36 Port: 16.6

Name	Current 15 Min.	Current Day	Current 15 Min.	Current Day
ES (Severely Error Seconds)	N/A	0	0	0
LOPS (Loss of Packet Sequence)	N/A	0	0	0
Late Packets	N/A	0	0	0
Early Packets	N/A	0	0	0
Lost Packets	N/A	0	0	0
Maximum Jitter	0	N/A	0	N/A
Average Jitter	0	N/A	0	N/A
Minimum Jitter	0	N/A	0	N/A
Packets Received	N/A	0	N/A	0
Bytes Received	N/A	N/A	N/A	0
Packets Sent	N/A	0	N/A	0
Bytes Sent	N/A	N/A	N/A	0

Valid Intervals: 0
Invalid Intervals: 0

```
Thu Nov 29 12:27:17 EST 2007 - Polling of RG_1195228536515 successful.
Thu Nov 29 12:27:16 EST 2007 - Polling of 10.52.30.36 successful.
```

FIGURE 16-150 CES-DS1 PMON Statistics Parameter Form - Port 2 on the iMG6x6MOD



CES-DS1 Port Management

Device: Customer_XYZ Port: 2 Device: 10.52.30.36 Port: 16.6

Hidden Statistics:

CES-DS1 15-min LCV
CES-DS1 15-min LES
CES-DS1 15-min LOSS
CES-DS1 15-min SES
CES-DS1 15-min UAS

Graphed Statistics (Maximum 6):

Saved Statistic Lists:

Display

● Absolute Values ○ Rate Per Second ○ Million Per Second

Polling Interval: 30

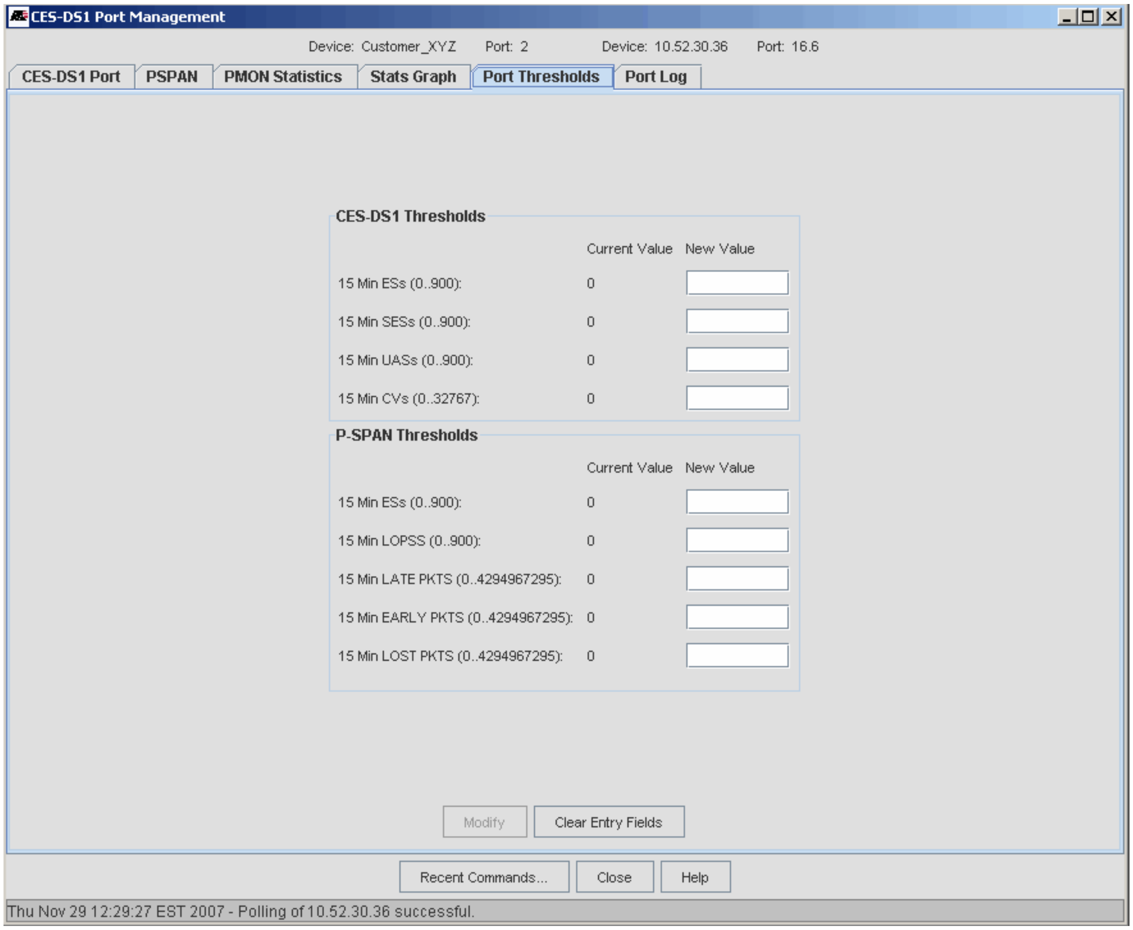
New Interval:

Note: Some historical data cannot be viewed when graphing absolute values

Thu Nov 29 12:28:44 EST 2007 - Polling of 10.52.30.36 successful.

FIGURE 16-151 CES-DS1 Graph Statistics Parameter Form - Port 2 on the iMG6x6MOD

Note: Only the CES8 Stats are currently available in graph format. Use the PMON Statistics tab for iMG statistics.



Device: Customer_XYZ Port: 2 Device: 10.52.30.36 Port: 16.6

CES-DS1 Thresholds

	Current Value	New Value
15 Min ESs (0..900):	0	
15 Min SESs (0..900):	0	
15 Min UASs (0..900):	0	
15 Min CVs (0..32767):	0	

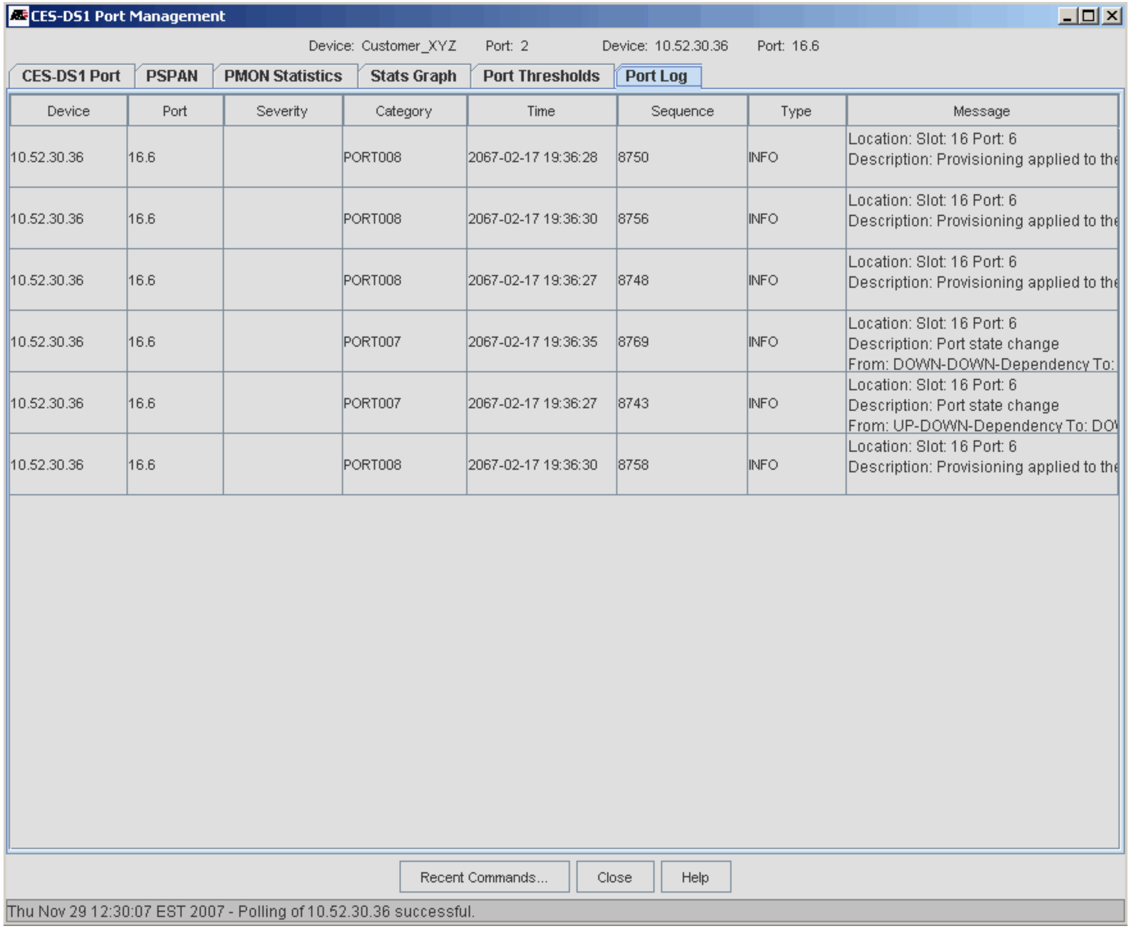
P-SPAN Thresholds

	Current Value	New Value
15 Min ESs (0..900):	0	
15 Min LOPSS (0..900):	0	
15 Min LATE PKTS (0..4294967295):	0	
15 Min EARLY PKTS (0..4294967295):	0	
15 Min LOST PKTS (0..4294967295):	0	

Thu Nov 29 12:29:27 EST 2007 - Polling of 10.52.30.36 successful.

FIGURE 16-152 CES-DS1 Port Thresholds Parameter Form - Port 2 on the iMG6x6MOD

Note: Only the CES8 thresholds appear. The iMG does not support thresholds that can be set.



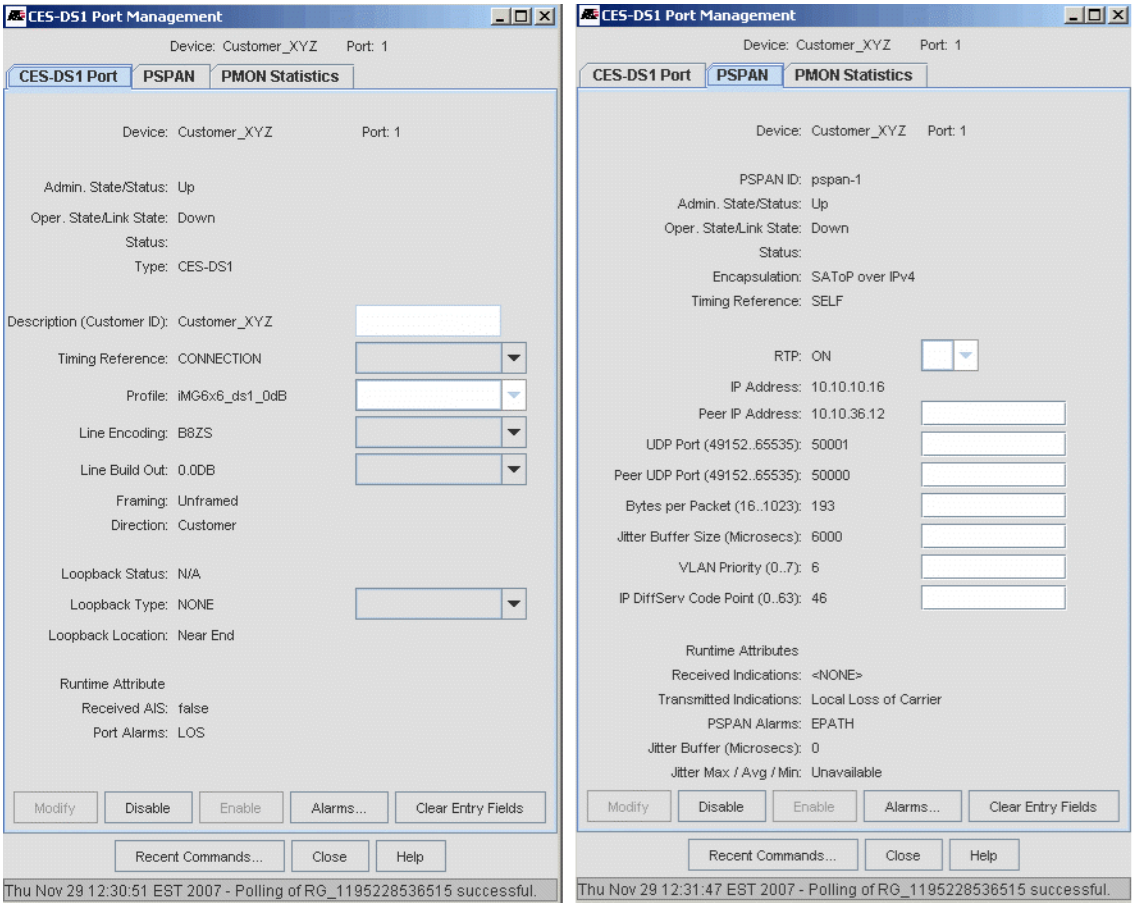
Device: Customer_XYZ Port: 2 Device: 10.52.30.36 Port: 16.6

Device	Port	Severity	Category	Time	Sequence	Type	Message
10.52.30.36	16.6		PORT008	2067-02-17 19:36:28	8750	INFO	Location: Slot: 16 Port: 6 Description: Provisioning applied to the
10.52.30.36	16.6		PORT008	2067-02-17 19:36:30	8756	INFO	Location: Slot: 16 Port: 6 Description: Provisioning applied to the
10.52.30.36	16.6		PORT008	2067-02-17 19:36:27	8748	INFO	Location: Slot: 16 Port: 6 Description: Provisioning applied to the
10.52.30.36	16.6		PORT007	2067-02-17 19:36:35	8769	INFO	Location: Slot: 16 Port: 6 Description: Port state change From: DOWN-DOWN-Dependency To:
10.52.30.36	16.6		PORT007	2067-02-17 19:36:27	8743	INFO	Location: Slot: 16 Port: 6 Description: Port state change From: UP-DOWN-Dependency To: DO
10.52.30.36	16.6		PORT008	2067-02-17 19:36:30	8758	INFO	Location: Slot: 16 Port: 6 Description: Provisioning applied to the

Thu Nov 29 12:30:07 EST 2007 - Polling of 10.52.30.36 successful.

FIGURE 16-153 CES-DS1 Port Log Parameter Form - Port 2 on the iMG6x6MOD

Note: Only the CES8 port logs appear. The iMG port does not support the Port Log feature.



Device: Customer_XYZ Port: 1

Device: Customer_XYZ Port: 1

Admin. State/Status: Up
Oper. State/Link State: Down
Status:
Type: CES-DS1

Description (Customer ID): Customer_XYZ
Timing Reference: CONNECTION
Profile: iMG6x6_ds1_0dB
Line Encoding: B8ZS
Line Build Out: 0.0DB
Framing: Unframed
Direction: Customer

Loopback Status: N/A
Loopback Type: NONE
Loopback Location: Near End

Runtime Attribute
Received AIS: false
Port Alarms: LOS

Thu Nov 29 12:30:51 EST 2007 - Polling of RG_1195228536515 successful.

Device: Customer_XYZ Port: 1

Device: Customer_XYZ Port: 1

PSPAN ID: pspan-1
Admin. State/Status: Up
Oper. State/Link State: Down
Status:
Encapsulation: SAToP over IPv4
Timing Reference: SELF

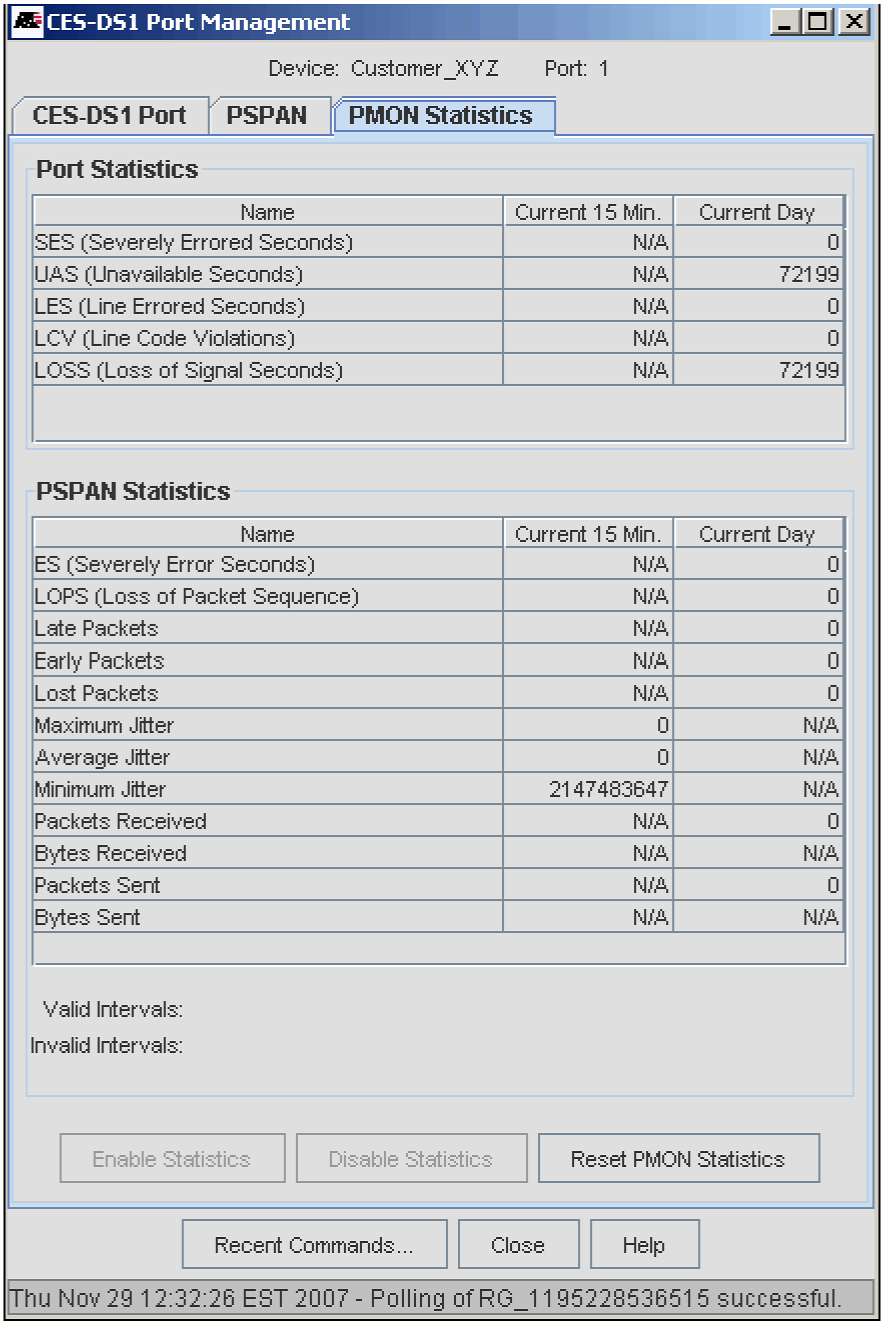
RTP: ON
IP Address: 10.10.10.16
Peer IP Address: 10.10.36.12
UDP Port (49152..65535): 50001
Peer UDP Port (49152..65535): 50000
Bytes per Packet (16..1023): 193
Jitter Buffer Size (Microsecs): 6000
VLAN Priority (0..7): 6
IP DiffServ Code Point (0..63): 46

Runtime Attributes
Received Indications: <NONE>
Transmitted Indications: Local Loss of Carrier
PSPAN Alarms: EPATH
Jitter Buffer (Microsecs): 0
Jitter Max / Avg / Min: Unavailable

Thu Nov 29 12:31:47 EST 2007 - Polling of RG_1195228536515 successful.

FIGURE 16-154 CES-DS1 Port and PSPAN Parameter Form - Port 1 on the iMG6x6MOD

Note: *In the example configuration, the peer end of Port 1 is not managed by the NMS. In this case, the one-sided screens will appear with the iMG supported tabs only.*



Device: Customer_XYZ Port: 1

Port Statistics

Name	Current 15 Min.	Current Day
SES (Severely Errored Seconds)	N/A	0
UAS (Unavailable Seconds)	N/A	72199
LES (Line Errored Seconds)	N/A	0
LCV (Line Code Violations)	N/A	0
LOSS (Loss of Signal Seconds)	N/A	72199

PSPAN Statistics

Name	Current 15 Min.	Current Day
ES (Severely Error Seconds)	N/A	0
LOPS (Loss of Packet Sequence)	N/A	0
Late Packets	N/A	0
Early Packets	N/A	0
Lost Packets	N/A	0
Maximum Jitter	0	N/A
Average Jitter	0	N/A
Minimum Jitter	2147483647	N/A
Packets Received	N/A	0
Bytes Received	N/A	N/A
Packets Sent	N/A	0
Bytes Sent	N/A	N/A

Valid Intervals:

Invalid Intervals:

Thu Nov 29 12:32:26 EST 2007 - Polling of RG_1195228536515 successful.

FIGURE 16-155 PMON Statistics Form - Port 1 on the iMG6x6MOD

16.14 NTE8 Dual Circuit Provisioning

In Release 7.0, the NTE8 card is used to allow DS1/E1 facilities to connect (backhaul) the ethernet network, with both ends of the DS1/E1 connections being on iMAP devices. Refer to the *Software Reference for iMAP Series Switches* for a complete description of the NTE8 configuration.

Note: Refer to "NTE8 Card" on page 389 and "NTE8 Port Management Form" on page 463 for an overview of the NTE8 card and DS1/E1 port attributes.

The NTE8 configuration always has dual endpoints, since there must be an iMAP 9000 device at each end. Moreover, each end must be correctly provisioned for the logical hierarchy (DS1, PPP, MLPP, ETH) of the NTE8. Finally, the hierarchy for each endpoint in a pair must be the same.

Configuring an MLPPP interface and its associated ETH interface is less straight-forward than the PPP interface, since the MLPPP can be associated with one or more ports. Since the MLPPP/PPP relationship has to be consistent at both ends of the DS1/E1 circuit, the user should configure both ends of the MLPPP (and its DS1/E1) connections at the same time.

The following figure shows an example configuration using DS1 ports. It includes a PPP-only as well as an MLPPP/PPPs configuration.

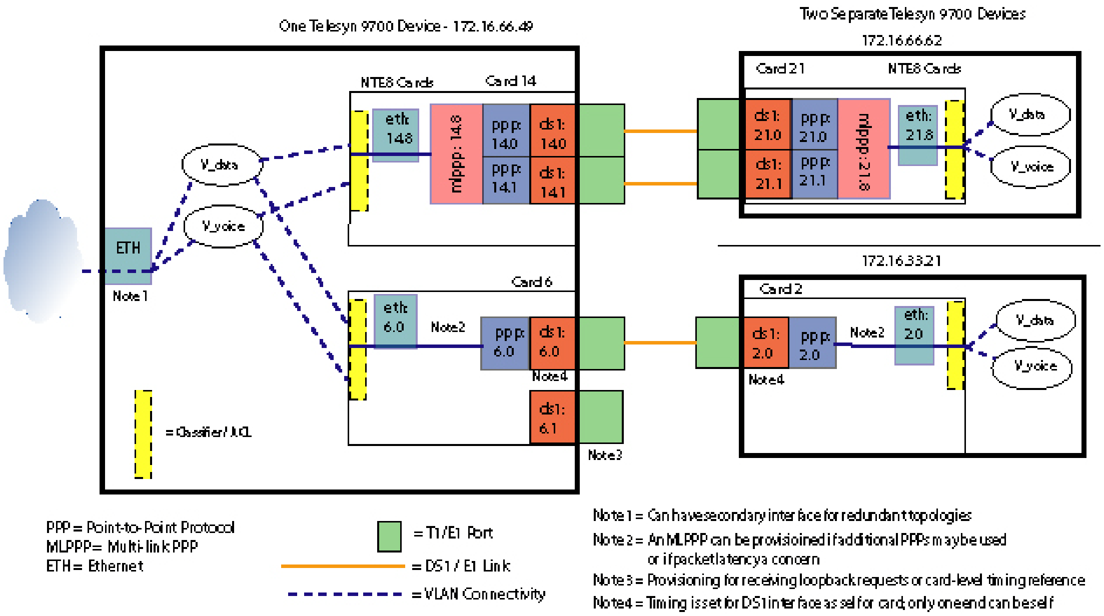

One Telesyn 9700 Device - 172.16.66.49
Two Separate Telesyn 9700 Devices
172.16.66.62
172.16.33.21
NTE8 Cards
Card 14
Card 21
NTE8 Cards
Card 6
Card 2
ETH
Note 1
V_data
V_voice
eth: 14.8
mlppp: 14.8
ppp: 14.0
ppp: 14.1
ds1: 14.0
ds1: 14.1
ds1: 21.0
ds1: 21.1
ppp: 21.0
ppp: 21.1
mlppp: 21.8
eth: 21.8
V_data
V_voice
eth: 6.0
Note2
ppp: 6.0
ds1: 6.0
Note4
ds1: 6.1
Note3
ds1: 2.0
ppp: 2.0
Note2
eth: 2.0
Note4
V_data
V_voice
= Classifier/ACL
PPP = Point-to-Point Protocol
MLPPP= Multi-link PPP
ETH= Ethernet
= T1/E1 Port
= DS1 / E1 Link
= VLAN Connectivity
Note 1 = Can have secondary interface for redundant topologies
Note 2 = An MLPPP can be provisioined if additional PPPs maybe used or if packet latency a concern
Note 3 = Provisioning for receiving loopback requests or card-level timing reference
Note4 = Timing is set for DS1 interface as self for card, only one end can be self

FIGURE 16-156 NTE Sample Configuration - Cards 5 and 1 used in Example

16.14.1 Main Provisioning Steps

The recommended steps for provisioning the NTE8 when there are no MLPPPs (PPPs only) are:

1. Create the NTE8 cards and provision them to support DS1.
2. Create a DS1/E1 port profile (refer to "Creating a Profile" on page 206).
3. Right click a device from the Physical Map and then *Provision -> Port Management.*
4. On the Port Management form, select an unprovisioned NTE8 port and select **Provision New Customer/Port**
5. On the Provision New NTE-DS1 Port form, create a useful Customer ID.
6. Set DS1 parameters by selecting a Port Profile. If you don’t use a profile, the default values will be used.
7. Fill in the Peer Port panel with the Device and Slot-Port to choose a far-end (“Z-end”) for the circuit.

Note: Since these DS1s are to be connected, the timing source is coordinated between them; if one end is set as SELF, the other end automatically changes to CARD.

8. Edit the PPP parameters, if desired. **These will be applied to both ends.**
9. Since this is for a PPP circuit, without MLPPP, do not edit the MLPPP interface parameters.
10. Select the VLAN that this PPP is to be connected to. *Note*: **the VLANs must already be configured.**
11. Press the Provision Button when complete.

The procedure for configuring an MLPPP for both ends is:

1. Create a PPP circuit as listed above, up to step 7.
2. Select an MLPPP Interface to use for the bundle.

Note: *The selection is constrained by MLPPP bundle consistency on both ends; once a PPP is associated with an MLPPP, the peer PPP must be associated with the peer MLPPP. This will become clear in the examples.*

16.14.2 Create/Provision NTE8 cards to Support DS1 Ports (Different Devices)

To create the cards (if this hasn't been done already), right click on the device and select *Provision -> Card Management*, which brings up the **Card Management Form**. Find the Slot (in this case 14) that is not provisioned, and select **Create Card**. Select the Profile as AutoProv if you wish the card to use the load that is in the AutoProv profile, the Admin State as UP (assuming you want the card to go into service), and the Ports Type as DS1. (If not explicitly chosen, DS1 is the default.) Click on **Create**, and the card status will change in the Card Management form to a Card Type of NTE8.

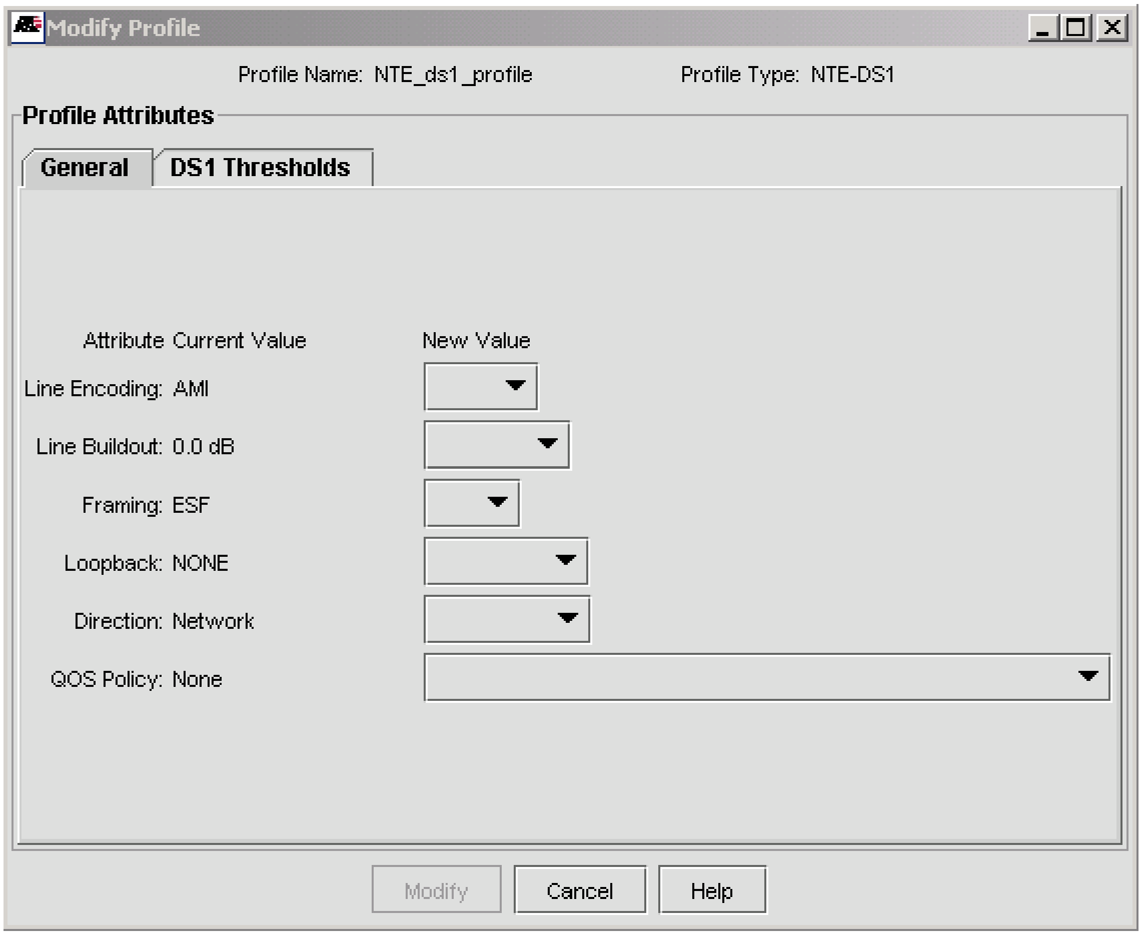
Note: *The card timing is initially Internal, as the only item in the pull-down. However, a DS1 port could be created that is connected to a system-wide, external timing source (with its timing source set to SELF). The user could then change the timing source for the card to that DS1 port.At this point you can download any NTE8 files if the Profile was set to Manually Provisioned.*

Note: *At this point, the card attribute Ports Type for the General Tab can be changed, but the card would need to be disabled, and there is a warning about the need to disable the card. The Profile can also be changed, and there is a warning that such a change will destroy existing provisioning data.*

16.14.3 Create DS1 Profile

When a DS1 port is provisioned, a DS1 profile must already exist so it can be associated with the DS1 port. In this example a profile called NTE_ds1_profile is created. The following figures show the profile has already been created and can be viewed in the Profile table by double-clicking on the profile row.

Note: *When a QoS Policy is applied to a DS1 port in the NTE8 configuration, it is actually applied to the ETH interface, which may contain one or more DS1/E1 interfaces. If different policies are applied to the multiple DS1s/E1s, the last policy applied will be applied to the ETH interface and therefore to all the DS1s/E1s.*

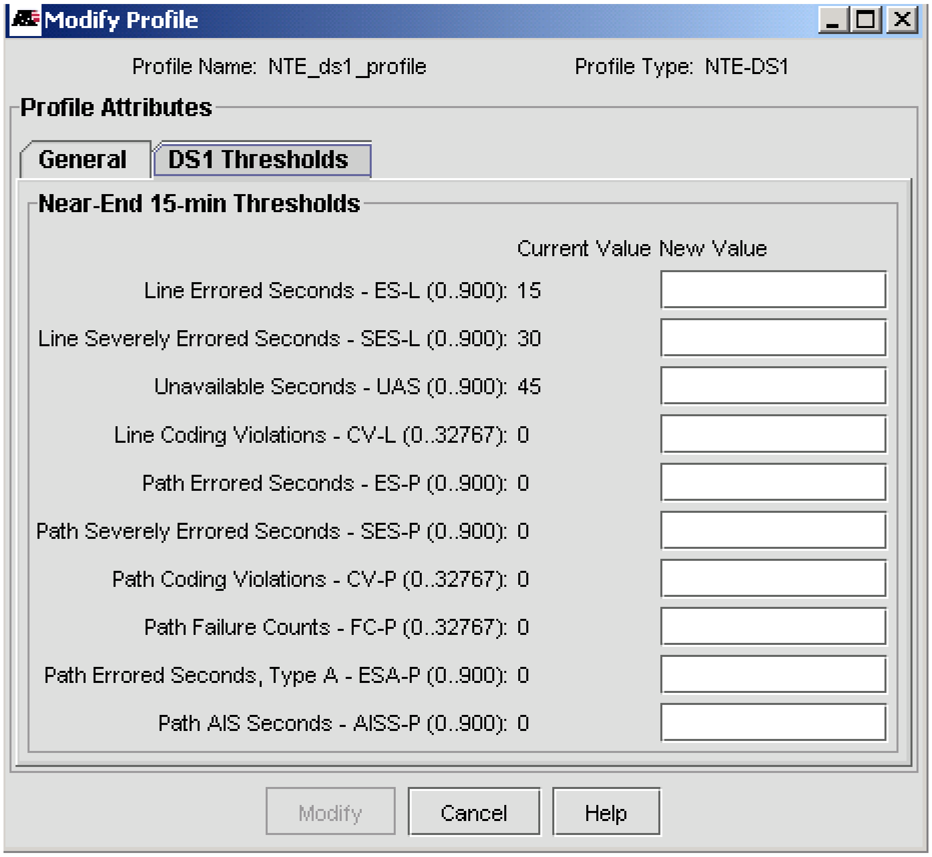


Profile Name: NTE_ds1_profile

Profile Type: NTE-DS1

Attribute	Current Value	New Value
Line Encoding:	AMI	
Line Buildout:	0.0 dB	
Framing:	ESF	
Loopback:	NONE	
Direction:	Network	
QOS Policy:	None	

FIGURE 16-157 Viewing DS1 Profile - General Tab



Modify Profile

Profile Name: NTE_ds1_profile Profile Type: NTE-DS1

Profile Attributes

Near-End 15-min Thresholds

	Current Value	New Value
Line Errored Seconds - ES-L (0..900):	15	
Line Severely Errored Seconds - SES-L (0..900):	30	
Unavailable Seconds - UAS (0..900):	45	
Line Coding Violations - CV-L (0..32767):	0	
Path Errored Seconds - ES-P (0..900):	0	
Path Severely Errored Seconds - SES-P (0..900):	0	
Path Coding Violations - CV-P (0..32767):	0	
Path Failure Counts - FC-P (0..32767):	0	
Path Errored Seconds, Type A - ESA-P (0..900):	0	
Path AIS Seconds - AISS-P (0..900):	0	

FIGURE 16-158 Viewing DS1 Profile - DS1 Thresholds Tab (Note non-0 values)

16.14.4 Provisioning one NTE8 Circuit

Selecting from the main menu *Tools -> Customer Management -> Add NTE DS1 Customer* brings up the **Provision New NTE-DS1 Port** Form. This is the form where the main task for Provisioning the NTE8 endpoints are done.

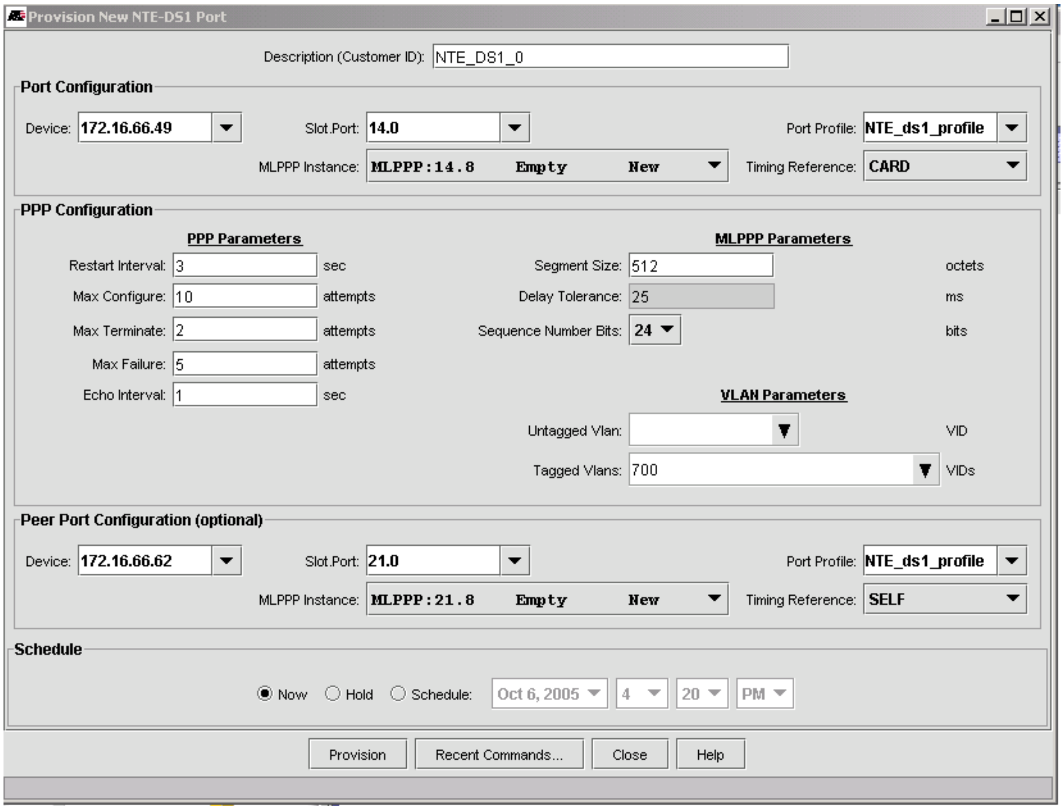
Note: You can also right click on the device and select Provision -> Port Management, and then on the Port Management form select an unprovisioned NTE8 port and click on Provision new Customer/Port. Note however that with these steps the device and port are already filled in and uneditable.

The device/ports available are the discovered DS1 ports in the managed network that are available for provisioning. Following are important points when filling out this form:

- You must input a Customer ID. When provisioning dual endpoints, this ID will be applied to both endpoints in the Port Inventory table. This allows immediate recognition of which ports are included in the dual configuration. The name should be descriptive so that users know this is part of a dual endpoint configuration.
- The Port Profiles used for each endpoint do not have to match, but care must be taken to ensure that the values are compatible.
- When the user selects an MLPPP instance for the near-end and is provisioning the MLPPP for the first time, the user selects an MLPPP that is EMPTY (No PPP members) and NEW (not yet created). (Adding a link to an already existing MLPPP is covered in the next subsection.)
- To provision the far end port, the user selects an appropriate device and port, and must select the MLPPP that can exist on the same card as the port. The example shows what is most common, with the 21.0 port being provisioned with the lowest number MLPPP available, 21.8.

- When the user clicks on **Provision**, the task completes, and the user selects **Yes** to continue data filling the form, the Customer ID field is cleared and the just provisioned ports are no longer available in the Port pull-down. Refer to the following figures.

Note: Any specified QoS Policy is applied tot he common Ethernet interface.



Provision New NTE-DS1 Port

Description (Customer ID): NTE_DS1_0

Port Configuration

Device: 172.16.66.49
Slot.Port: 14.0
Port Profile: NTE_ds1_profile
MLPPP Instance: MLPPP:14.8 Empty New
Timing Reference: CARD

PPP Configuration

PPP Parameters

Restart Interval: 3 sec
Max Configure: 10 attempts
Max Terminate: 2 attempts
Max Failure: 5 attempts
Echo Interval: 1 sec

MLPPP Parameters

Segment Size: 512 octets
Delay Tolerance: 25 ms
Sequence Number Bits: 24 bits

VLAN Parameters

Untagged Vlan: VID
Tagged Vlans: 700 VIDs

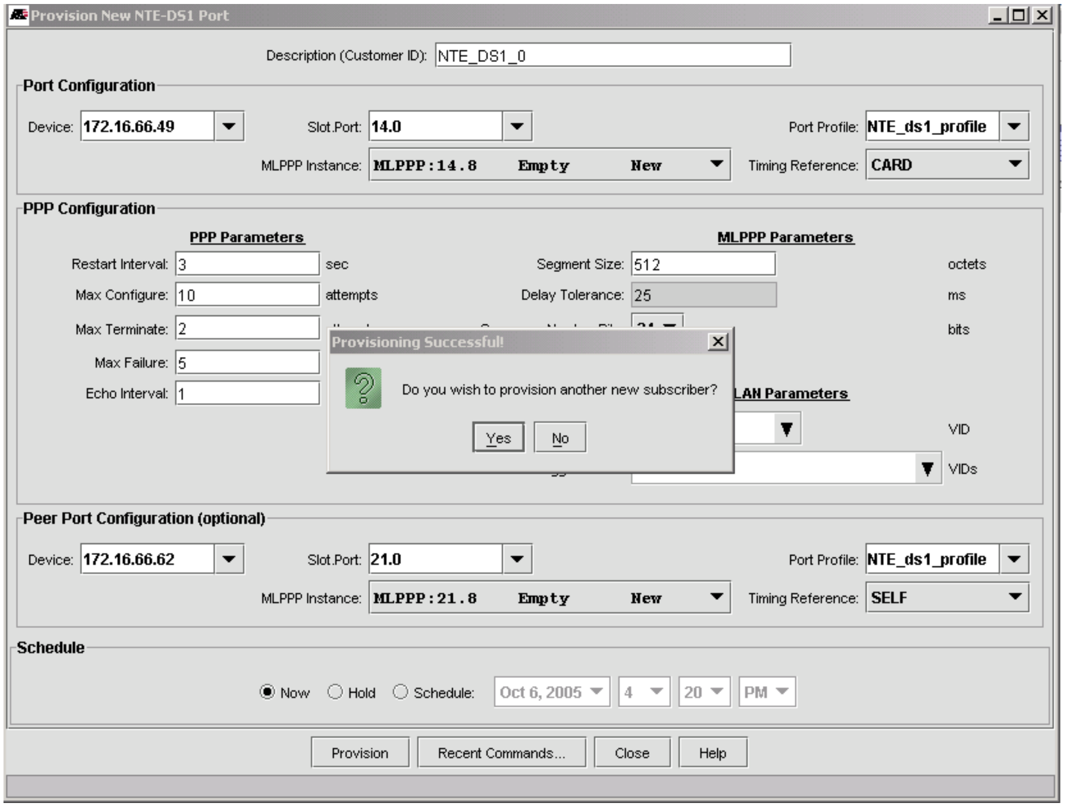
Peer Port Configuration (optional)

Device: 172.16.66.62
Slot.Port: 21.0
Port Profile: NTE_ds1_profile
MLPPP Instance: MLPPP:21.8 Empty New
Timing Reference: SELF

Schedule

● Now ○ Hold ○ Schedule: Oct 6, 2005 4 20 PM

FIGURE 16-159 Provision a New NTE-DS1 Port (MLPPP)


Provision New NTE-DS1 Port

Description (Customer ID): NTE_DS1_0

Port Configuration

Device: 172.16.66.49 Slot.Port: 14.0 Port Profile: NTE_ds1_profile

MLPPP Instance: MLPPP:14.8 Empty New Timing Reference: CARD

PPP Configuration

PPP Parameters			MLPPP Parameters		
Restart Interval:	3	sec	Segment Size:	512	octets
Max Configure:	10	attempts	Delay Tolerance:	25	ms
Max Terminate:	2				bits
Max Failure:	5				
Echo Interval:	1				

LAN Parameters

VID

VIDs

Provisioning Successful!

Do you wish to provision another new subscriber?

Peer Port Configuration (optional)

Device: 172.16.66.62 Slot.Port: 21.0 Port Profile: NTE_ds1_profile

MLPPP Instance: MLPPP:21.8 Empty New Timing Reference: SELF

Schedule

● Now ○ Hold ○ Schedule: Oct 6, 2005 4 20 PM

FIGURE 16-160 Result of Success (Fields Ready for next Customer)

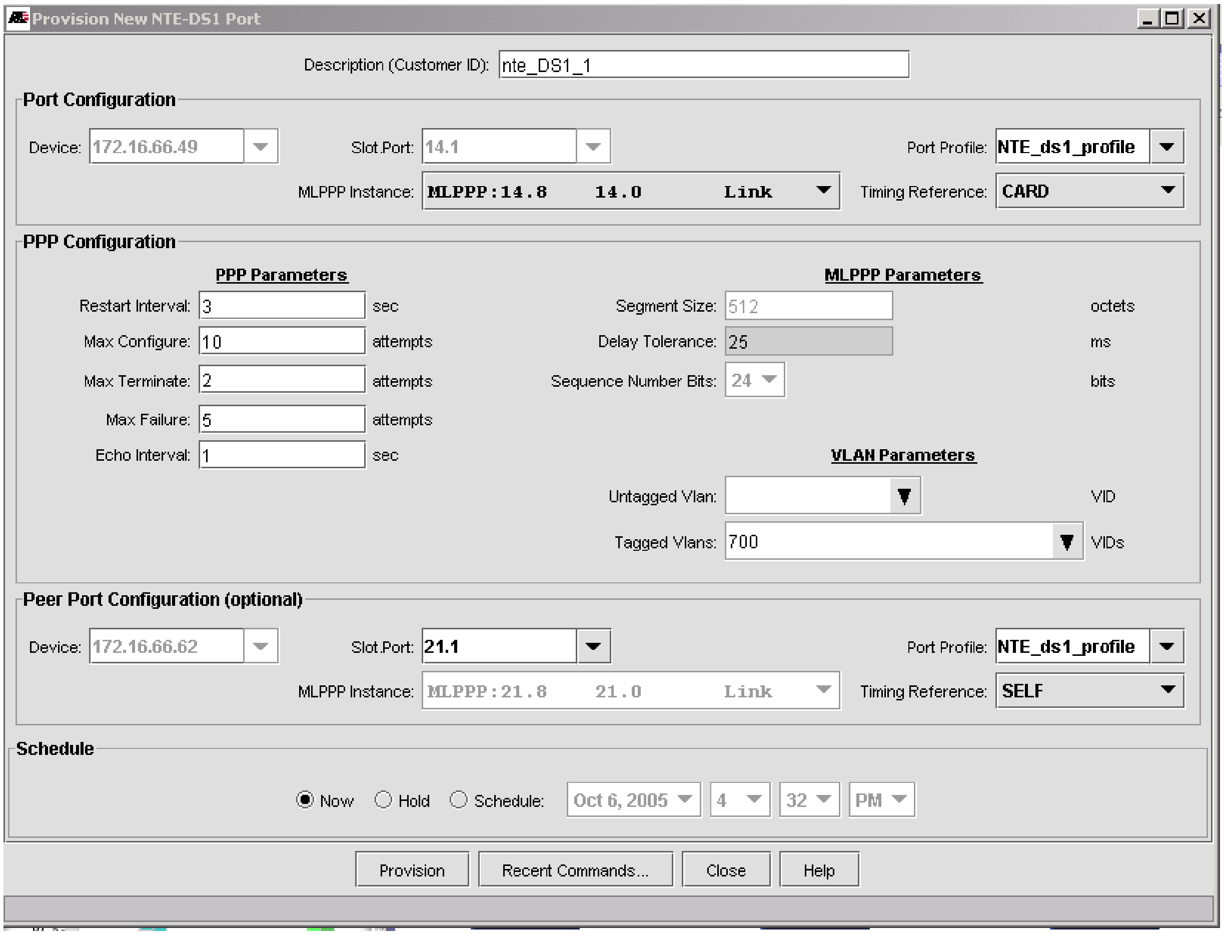
16.14.5 Adding PPPs to the MLPPP

Once the NTE8 DS1 circuit has been set up, with a PPP and associated MLPPP at each end, the user can add DS1s/PPPs to the existing MLPPPs. By filling out the NTE provisioning forms, the user can ensure the provisioning goes smoothly and the correct parameters are entered.

Refer to the following figure while reading below.

To provision the second DS1s/PPPs, right click on the relevant device, in this case the .49 device, and select *Provision -> Port Management*. In the Port Management form, select the DS1 that is going to be added (in this case, 14.1). This PPP is being added to MLPPP 14.8, so the user chooses this MLPPP from the pull-down. Note that the MLPPP already contains the PPP 14.0 and has already been configured (LINK).

Once the user chooses this MLPPP, the peer MLPPP is **automatically** datafilled in, since in any set of PPP pairs, the PPPs on one side must have the same peer MLPPP.



Description (Customer ID): nte_DS1_1

Port Configuration

Device: 172.16.66.49
Slot.Port: 14.1
Port Profile: NTE_ds1_profile
MLPPP Instance: MLPPP:14.8 14.0 Link
Timing Reference: CARD

PPP Configuration

PPP Parameters

Restart Interval:	3	sec
Max Configure:	10	attempts
Max Terminate:	2	attempts
Max Failure:	5	attempts
Echo Interval:	1	sec

MLPPP Parameters

Segment Size:	512	octets
Delay Tolerance:	25	ms
Sequence Number Bits:	24	bits

VLAN Parameters

Untagged Vlan:		VID
Tagged Vlans:	700	VIDs

Peer Port Configuration (optional)

Device: 172.16.66.62
Slot.Port: 21.1
Port Profile: NTE_ds1_profile
MLPPP Instance: MLPPP:21.8 21.0 Link
Timing Reference: SELF

Schedule

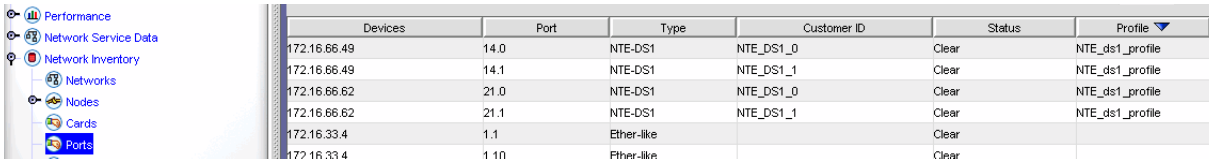
● Now ○ Hold ○ Schedule: Oct 6, 2005 4 32 PM

FIGURE 16-161 Provision New NTE-DS1 Port - Dual PPP

16.14.6 Viewing Provisioning Results - Port Inventory Table

To see the results of the dual endpoint provisioning, go to the Port Inventory window and sort on the Customer ID. The two ports are placed together since they share the same Customer ID. Refer to the following figure.

Note: *The user can also go to the Port Management window for the device and sort on Customer ID.*



Devices	Port	Type	Customer ID	Status	Profile ▼
172.16.66.49	14.0	NTE-DS1	NTE_DS1_0	Clear	NTE_ds1_profile
172.16.66.49	14.1	NTE-DS1	NTE_DS1_1	Clear	NTE_ds1_profile
172.16.66.62	21.0	NTE-DS1	NTE_DS1_0	Clear	NTE_ds1_profile
172.16.66.62	21.1	NTE-DS1	NTE_DS1_1	Clear	NTE_ds1_profile
172.16.33.4	1.1	Ether-like		Clear	
172.16.33.4	1.10	Ether-like		Clear	

FIGURE 16-162 Viewing Dual Endpoints on Port Management - Same Customer ID on Different Devices

This shows that ports 14.0 and 21.0 are the endpoints of one pair (Customer ID NTE_DS1_0) and ports 14.1 and 21.1 are the endpoints of the other pair (Customer ID NTE_DS1_1). By double-clicking on either of these rows, the DS1 Port Management tabbed form appears, with the selected port on the left. One can then view/modify the details of the configuration.

Note: *In this tabbed form, it is possible to change the attributes of the endpoints, However, in most cases the user should plan the dual endpoints so that configuration is easy and less prone to error.*

16.14.7 Viewing Provisioning Results - Port Details Form

16.14.7.1 DS1 Port Tab

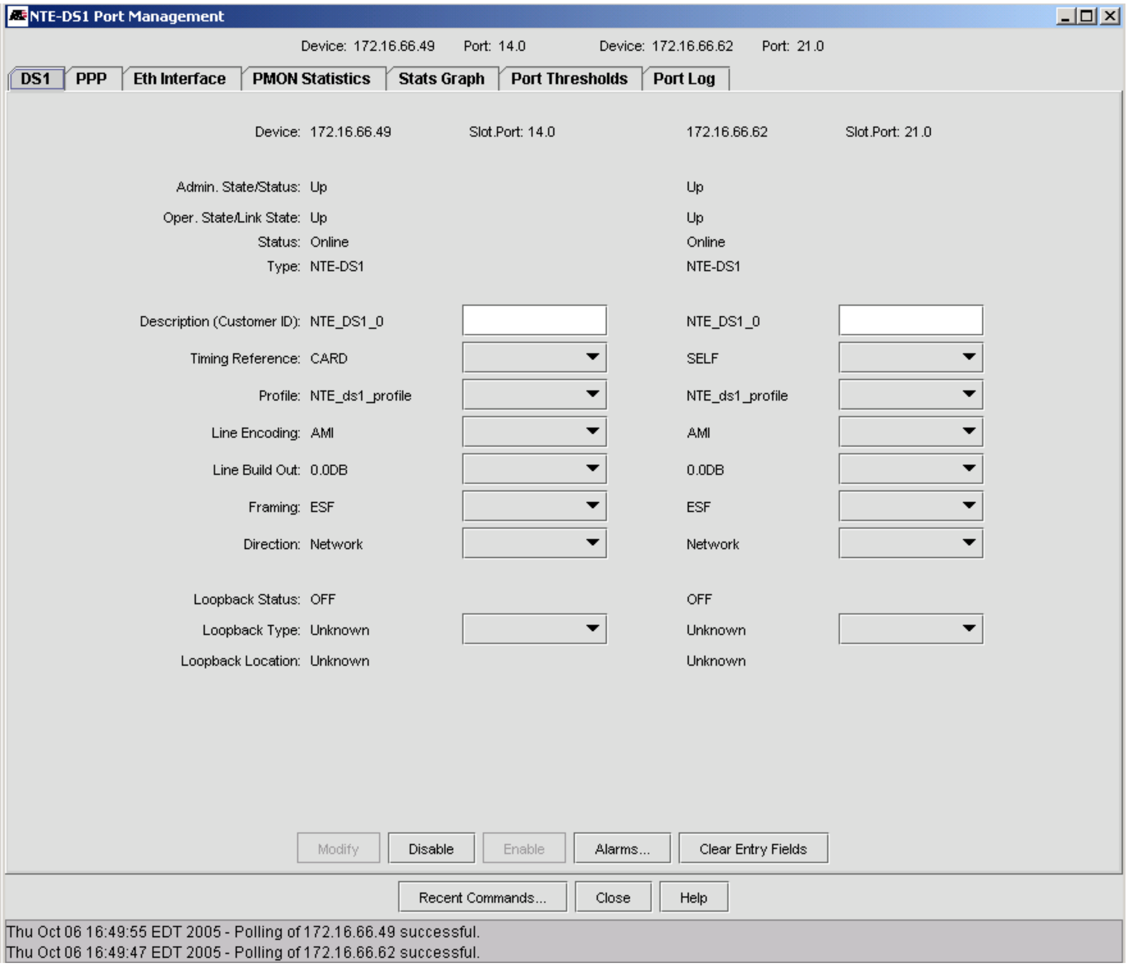
The following figure shows the Port Management form that appears when the user double-clicks on port 14.0 in the Port Inventory Form.

The port 14.0 is on the left, since that is the row that was selected; if the user selected 21.0 on the other device, port 21.0 would appear on the left.

The user can change attributes that are part of the Profile, but after clicking on Modify the user would see the Profile with an "*" next to it, meaning the Profile is out-of-sync. (This would also show up in the port inventory table.) The user would need to re-apply the profile make the '*' disappear.

The user can change the Description (Customer ID), but that would disassociate the two endpoints.

Note: *The DS1 tab shows only the implicit connection between the endpoints; it is the PPP tab that explicitly ties the two endpoints together, discussed below.*



Device: 172.16.66.49 Port: 14.0 Device: 172.16.66.62 Port: 21.0

Device:	172.16.66.49	Slot.Port: 14.0	172.16.66.62	Slot.Port: 21.0
Admin. State/Status:	Up		Up	
Oper. State/Link State:	Up		Up	
Status:	Online		Online	
Type:	NTE-DS1		NTE-DS1	
Description (Customer ID):	NTE_DS1_0		NTE_DS1_0	
Timing Reference:	CARD		SELF	
Profile:	NTE_ds1_profile		NTE_ds1_profile	
Line Encoding:	AMI		AMI	
Line Build Out:	0.0DB		0.0DB	
Framing:	ESF		ESF	
Direction:	Network		Network	
Loopback Status:	OFF		OFF	
Loopback Type:	Unknown		Unknown	
Loopback Location:	Unknown		Unknown	

```
Thu Oct 06 16:49:55 EDT 2005 - Polling of 172.16.66.49 successful.
Thu Oct 06 16:49:47 EDT 2005 - Polling of 172.16.66.62 successful.
```

FIGURE 16-163 DS1 Tab for NTE Example

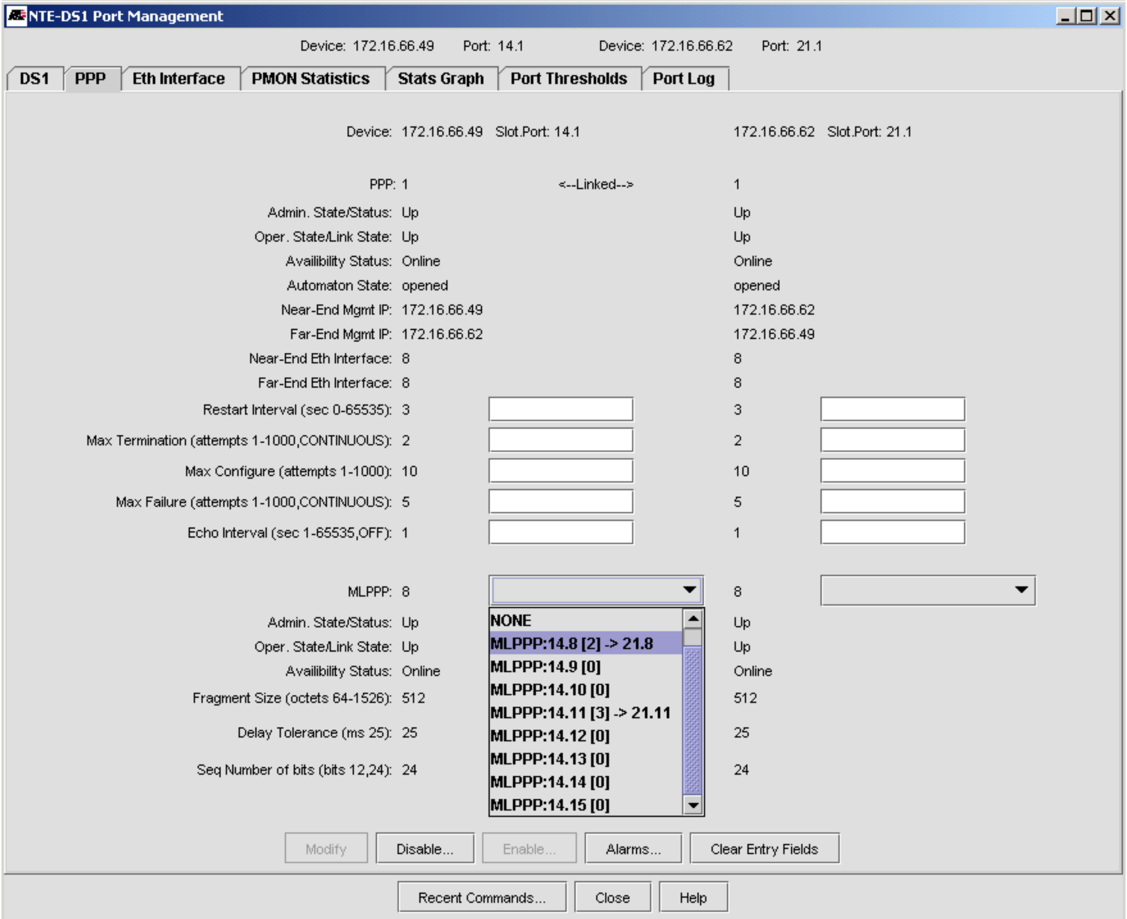
16.14.7.2 PPP Tab

The following figure shows the PPP tab for the two endpoints.

As with the DS1 tab, the row selected is the port that appears on the left.

The main attributes of the PPPs are at the top of the form and are read only.

Note that the pull-down for the MLPPP includes the currently configured MLPPP and its connection to its peer MLPPP (MLPPP 21.8).



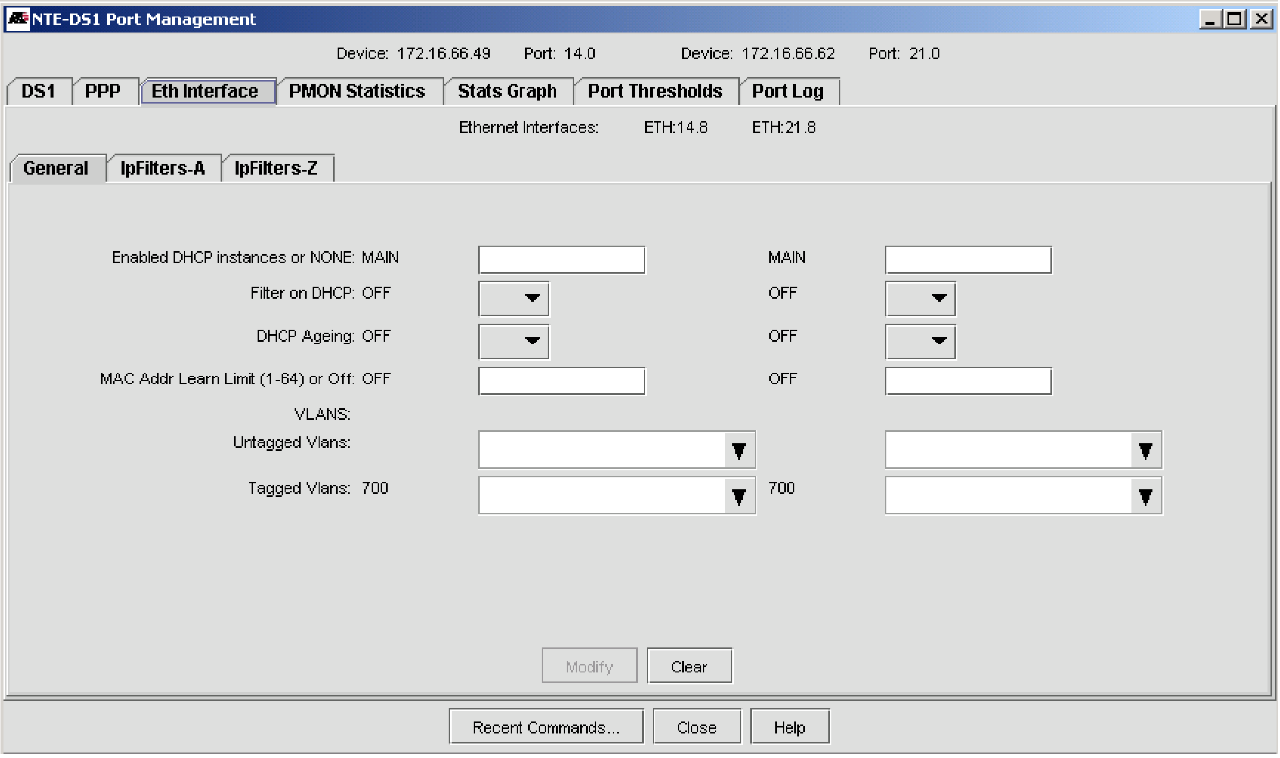
Device: 172.16.66.49 Port: 14.1 Device: 172.16.66.62 Port: 21.1

Device:	172.16.66.49 Slot.Port: 14.1	172.16.66.62 Slot.Port: 21.1
PPP:	1 <--Linked-->	1
Admin. State/Status:	Up	Up
Oper. State/Link State:	Up	Up
Availibility Status:	Online	Online
Automaton State:	opened	opened
Near-End Mgmt IP:	172.16.66.49	172.16.66.62
Far-End Mgmt IP:	172.16.66.62	172.16.66.49
Near-End Eth Interface:	8	8
Far-End Eth Interface:	8	8
Restart Interval (sec 0-65535):	3	3
Max Termination (attempts 1-1000,CONTINUOUS):	2	2
Max Configure (attempts 1-1000):	10	10
Max Failure (attempts 1-1000,CONTINUOUS):	5	5
Echo Interval (sec 1-65535,OFF):	1	1
MLPPP:	8	8
Admin. State/Status:	Up	Up
Oper. State/Link State:	Up	Up
Availibility Status:	Online	Online
Fragment Size (octets 64-1526):	512	512
Delay Tolerance (ms 25):	25	25
Seq Number of bits (bits 12,24):	24	24

NONE
MLPPP:14.8 [2] -> 21.8
MLPPP:14.9 [0]
MLPPP:14.10 [0]
MLPPP:14.11 [3] -> 21.11
MLPPP:14.12 [0]
MLPPP:14.13 [0]
MLPPP:14.14 [0]
MLPPP:14.15 [0]

FIGURE 16-164 PPP Tab for NTE Example

16.14.7.3 Eth Interface Tab



Device: 172.16.66.49 Port: 14.0 Device: 172.16.66.62 Port: 21.0

Ethernet Interfaces: ETH:14.8 ETH:21.8

Enabled DHCP instances or NONE:	MAIN		MAIN	
Filter on DHCP:	OFF		OFF	
DHCP Ageing:	OFF		OFF	
MAC Addr Learn Limit (1-64) or Off:	OFF		OFF	
VLANS:				
Untagged Vlans:				
Tagged Vlans:	700		700	

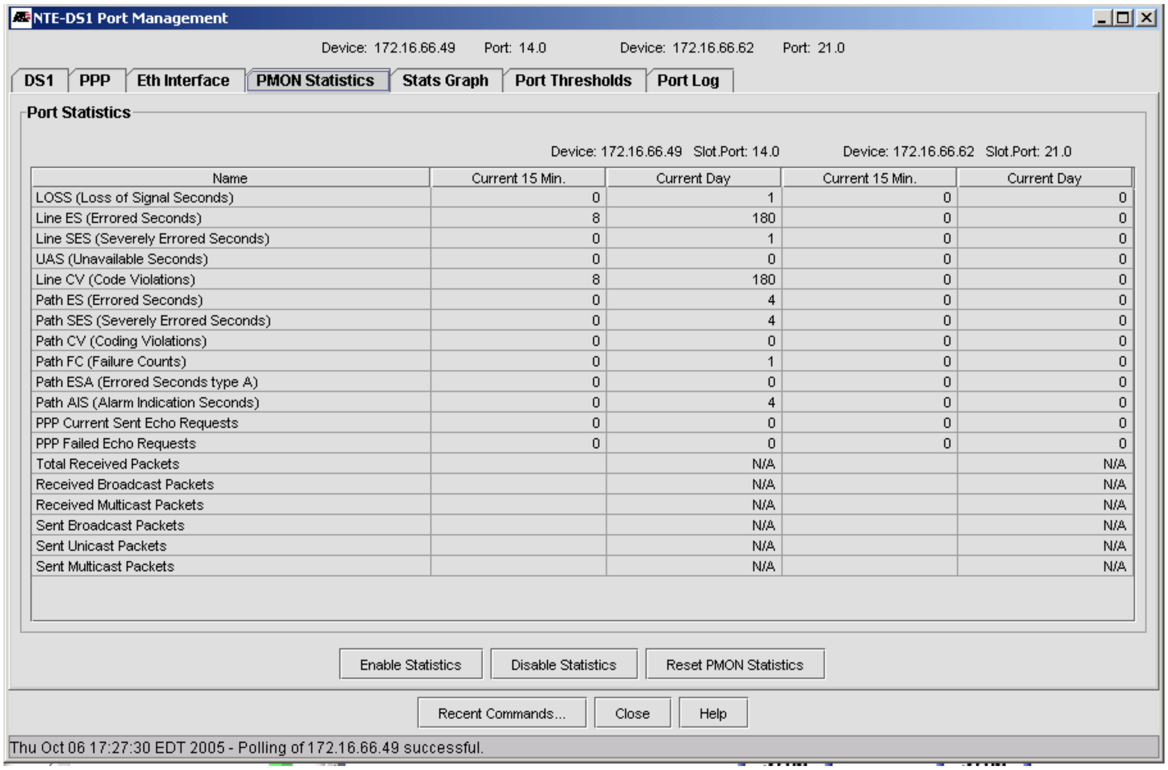
FIGURE 16-165 Eth Interface tab for NTE Example

16.14.7.4 PMON Statistics Tab

This tab shows the PMON Statistics tab. Refer to the following figure.

Note that the table lists the 14.0 and 21.0 Port statistics together.

When the user presses the function buttons (Enable, Disable, etc.), they are applied to **both** ports.



	Device: 172.16.66.49 Slot.Port: 14.0		Device: 172.16.66.62 Slot.Port: 21.0	
Name	Current 15 Min.	Current Day	Current 15 Min.	Current Day
LOSS (Loss of Signal Seconds)	0	1	0	0
Line ES (Errored Seconds)	8	180	0	0
Line SES (Severely Errored Seconds)	0	1	0	0
UAS (Unavailable Seconds)	0	0	0	0
Line CV (Code Violations)	8	180	0	0
Path ES (Errored Seconds)	0	4	0	0
Path SES (Severely Errored Seconds)	0	4	0	0
Path CV (Coding Violations)	0	0	0	0
Path FC (Failure Counts)	0	1	0	0
Path ESA (Errored Seconds type A)	0	0	0	0
Path AIS (Alarm Indication Seconds)	0	4	0	0
PPP Current Sent Echo Requests	0	0	0	0
PPP Failed Echo Requests	0	0	0	0
Total Received Packets		N/A		N/A
Received Broadcast Packets		N/A		N/A
Received Multicast Packets		N/A		N/A
Sent Broadcast Packets		N/A		N/A
Sent Unicast Packets		N/A		N/A
Sent Multicast Packets		N/A		N/A

Thu Oct 06 17:27:30 EDT 2005 - Polling of 172.16.66.49 successful.

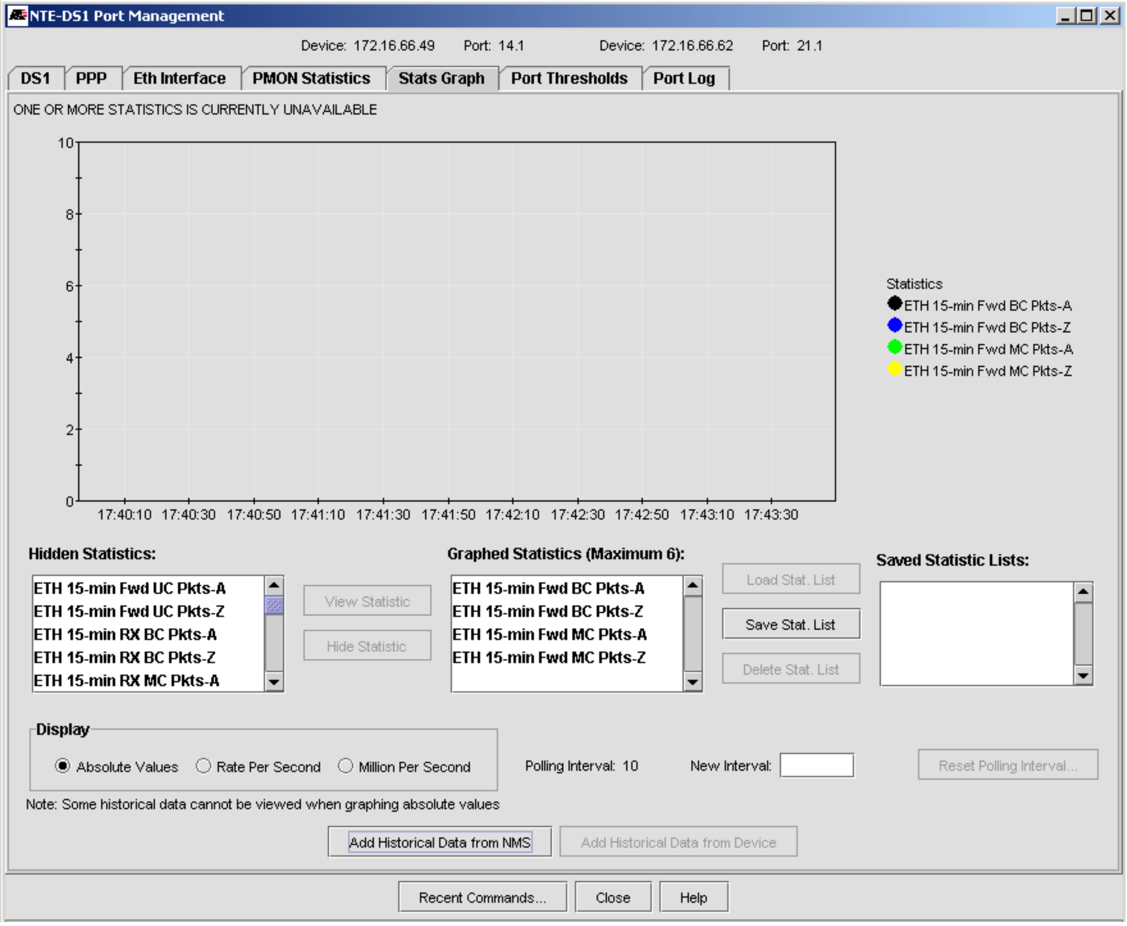
FIGURE 16-166 PMON Statistics Tab for two Endpoints

16.14.7.5 Stats Graph Tab

This form makes graphs of the statistics and allows the stats used to be saved as a list and reloaded later. Refer to the following figure.

Note: *The statistics for each endpoint have the suffix -A or -Z to identify each one. The -A is the port on the left side of the two ports shown at the top of the form, and the -Z is the right side.*

Note: *The statistics counters may need to be enabled first on the device. This is done from the PMON Statistics tab, described in "PMON Statistics Tab" on page 665.*



NTE-DS1 Port Management

Device: 172.16.66.49 Port: 14.1 Device: 172.16.66.62 Port: 21.1

ONE OR MORE STATISTICS IS CURRENTLY UNAVAILABLE

Hidden Statistics:
ETH 15-min Fwd UC Pkts-A
ETH 15-min Fwd UC Pkts-Z
ETH 15-min RX BC Pkts-A
ETH 15-min RX BC Pkts-Z
ETH 15-min RX MC Pkts-A

Graphed Statistics (Maximum 6):
ETH 15-min Fwd BC Pkts-A
ETH 15-min Fwd BC Pkts-Z
ETH 15-min Fwd MC Pkts-A
ETH 15-min Fwd MC Pkts-Z

Saved Statistic Lists:

Display
● Absolute Values ○ Rate Per Second ○ Million Per Second

Polling Interval: 10 New Interval:

Note: Some historical data cannot be viewed when graphing absolute values

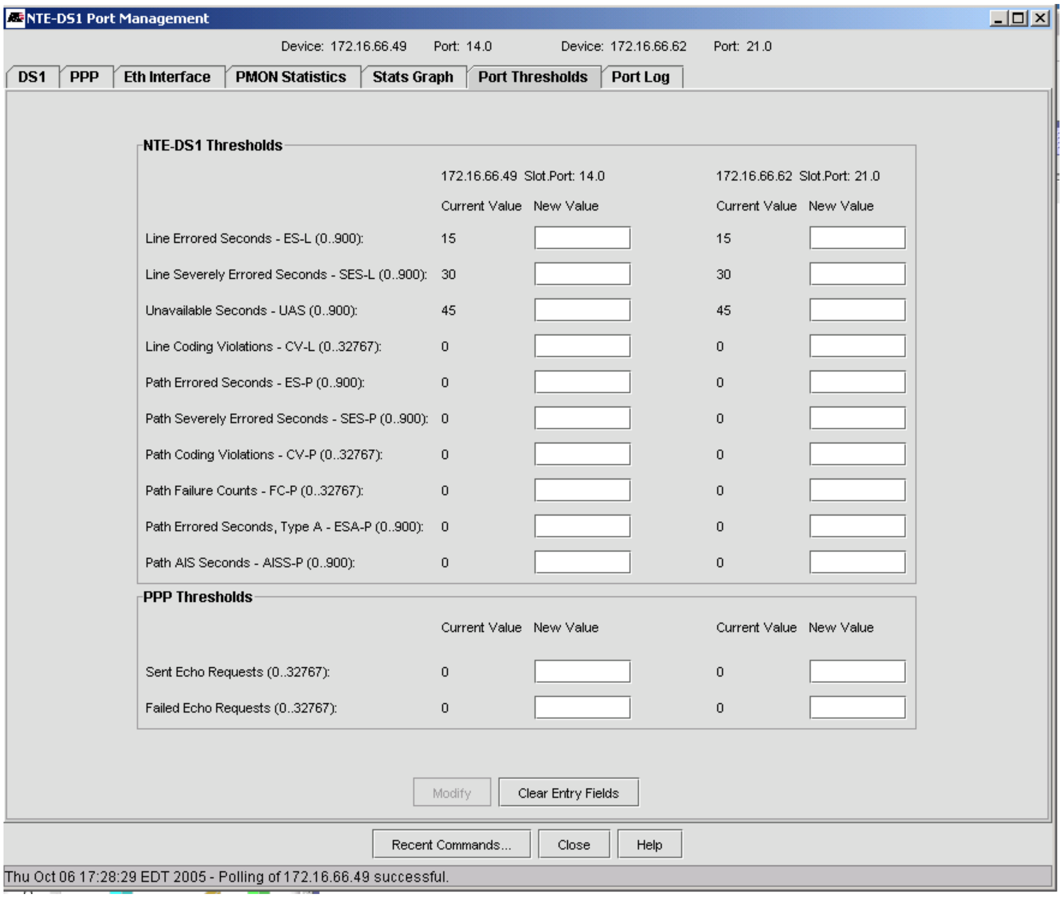
Reset Polling Interval...
Add Historical Data from NMS
Add Historical Data from Device
Recent Commands...
Close
Help

FIGURE 16-167 Stats Graph Tab for two Endpoints

16.14.7.6 Port Thresholds Tab

This form allows the user to modify the threshold values for the DS1/E1 and PPP statisitcs.When a new value is entered in the New Value field, the Modify button is enabled. These thresholds are set on the device and when crossed will cause thresholds crossing traps to be sent to the AlliedView NMS. These are displayed in the Event/Alarm tables.

Note: *In most cases, the DS1/E1 values are not modified because they are part of the DS1/E1 port profile; if the user does change a value, the port is now out of sync with its associated profile, and an "*" will appear next to the Profile name on the DS1/E1 Port tab form (as well as the Port Inventory table). In the dual endpoint configuration, the "*" will appear next to the specific port where the values were changed from the Profile. To Resync the port, the user must re-apply the profile on the DS1/E1 tab form, which puts the values back to what they are in the Profile.*



Device: 172.16.66.49 Port: 14.0 Device: 172.16.66.62 Port: 21.0

NTE-DS1 Thresholds

	172.16.66.49 Slot.Port: 14.0		172.16.66.62 Slot.Port: 21.0	
	Current Value	New Value	Current Value	New Value
Line Errored Seconds - ES-L (0..900):	15		15	
Line Severely Errored Seconds - SES-L (0..900):	30		30	
Unavailable Seconds - UAS (0..900):	45		45	
Line Coding Violations - CV-L (0..32767):	0		0	
Path Errored Seconds - ES-P (0..900):	0		0	
Path Severely Errored Seconds - SES-P (0..900):	0		0	
Path Coding Violations - CV-P (0..32767):	0		0	
Path Failure Counts - FC-P (0..32767):	0		0	
Path Errored Seconds, Type A - ESA-P (0..900):	0		0	
Path AIS Seconds - AISS-P (0..900):	0		0	

PPP Thresholds

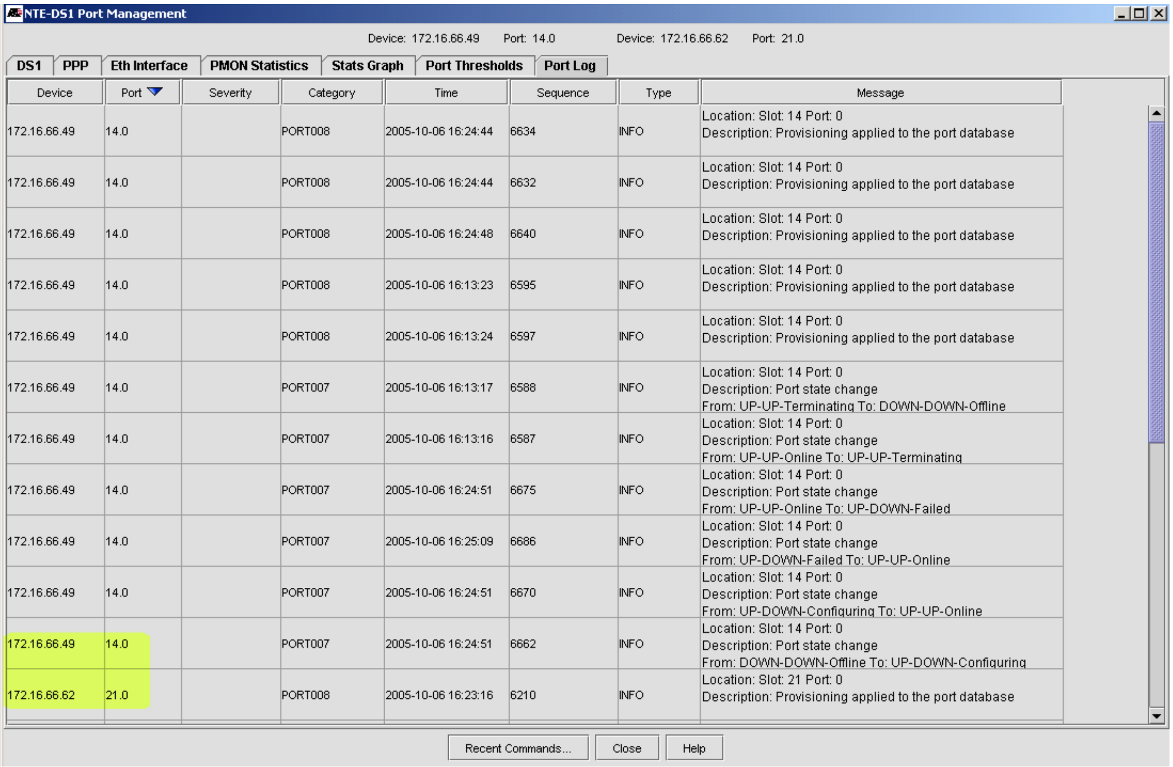
	Current Value	New Value	Current Value	New Value
Sent Echo Requests (0..32767):	0		0	
Failed Echo Requests (0..32767):	0		0	

Thu Oct 06 17:28:29 EDT 2005 - Polling of 172.16.66.49 successful.

FIGURE 16-168 Port Thresholds Graph Tab for two Endpoints

16.14.7.7 Port Log Tag

The following figure shows the Port Log tab for the two endpoints. These entries are derived from the Syslog system.



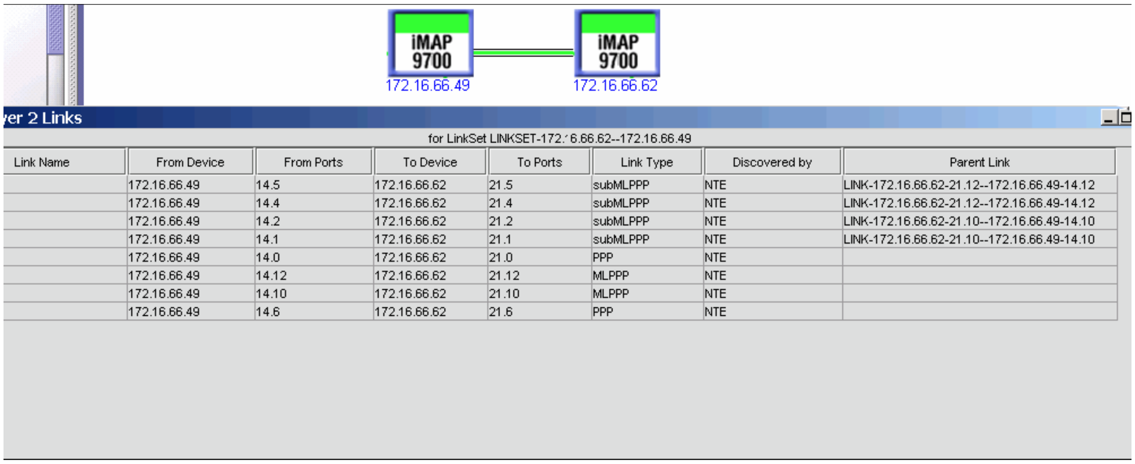
Device	Port	Severity	Category	Time	Sequence	Type	Message
172.16.66.49	14.0		PORT008	2005-10-06 16:24:44	6634	INFO	Location: Slot: 14 Port: 0 Description: Provisioning applied to the port database
172.16.66.49	14.0		PORT008	2005-10-06 16:24:44	6632	INFO	Location: Slot: 14 Port: 0 Description: Provisioning applied to the port database
172.16.66.49	14.0		PORT008	2005-10-06 16:24:48	6640	INFO	Location: Slot: 14 Port: 0 Description: Provisioning applied to the port database
172.16.66.49	14.0		PORT008	2005-10-06 16:13:23	6595	INFO	Location: Slot: 14 Port: 0 Description: Provisioning applied to the port database
172.16.66.49	14.0		PORT008	2005-10-06 16:13:24	6597	INFO	Location: Slot: 14 Port: 0 Description: Provisioning applied to the port database
172.16.66.49	14.0		PORT007	2005-10-06 16:13:17	6588	INFO	Location: Slot: 14 Port: 0 Description: Port state change From: UP-UP-Terminating To: DOWN-DOWN-Offline
172.16.66.49	14.0		PORT007	2005-10-06 16:13:16	6587	INFO	Location: Slot: 14 Port: 0 Description: Port state change From: UP-UP-Online To: UP-UP-Terminating
172.16.66.49	14.0		PORT007	2005-10-06 16:24:51	6675	INFO	Location: Slot: 14 Port: 0 Description: Port state change From: UP-UP-Online To: UP-DOWN-Failed
172.16.66.49	14.0		PORT007	2005-10-06 16:25:09	6686	INFO	Location: Slot: 14 Port: 0 Description: Port state change From: UP-DOWN-Failed To: UP-UP-Online
172.16.66.49	14.0		PORT007	2005-10-06 16:24:51	6670	INFO	Location: Slot: 14 Port: 0 Description: Port state change From: UP-DOWN-Configuring To: UP-UP-Online
172.16.66.49	14.0		PORT007	2005-10-06 16:24:51	6662	INFO	Location: Slot: 14 Port: 0 Description: Port state change From: DOWN-DOWN-Offline To: UP-DOWN-Configuring
172.16.66.62	21.0		PORT008	2005-10-06 16:23:16	6210	INFO	Location: Slot: 21 Port: 0 Description: Provisioning applied to the port database

FIGURE 16-169 Port Log Tab for two Endpoints

16.14.8 Viewing NTE8 Endpoints on Physical Map

Creation of PPP or MLPPP circuits through the NMS (or through CLI, directly) will trigger a discovery process on the devices so that they will know which Device and Port is currently at their far-end. This information is collected during NMS discovery of devices and will generate appropriate links on the Physical and VLAN maps, showing VLAN connectivity.

The following figure shows the Physical map and the physical link between the .20 and .18 devices. Double-clicking on the link brings up the Layer 2 Links table, and which includes all the link types (DS1. PPP, and MLPPP) that are included.



for LinkSet LINKSET-172.'6.66.62--172.16.66.49

Link Name	From Device	From Ports	To Device	To Ports	Link Type	Discovered by	Parent Link
	172.16.66.49	14.5	172.16.66.62	21.5	subMLPPP	NTE	LINK-172.16.66.62-21.12--172.16.66.49-14.12
	172.16.66.49	14.4	172.16.66.62	21.4	subMLPPP	NTE	LINK-172.16.66.62-21.12--172.16.66.49-14.12
	172.16.66.49	14.2	172.16.66.62	21.2	subMLPPP	NTE	LINK-172.16.66.62-21.10--172.16.66.49-14.10
	172.16.66.49	14.1	172.16.66.62	21.1	subMLPPP	NTE	LINK-172.16.66.62-21.10--172.16.66.49-14.10
	172.16.66.49	14.0	172.16.66.62	21.0	PPP	NTE	
	172.16.66.49	14.12	172.16.66.62	21.12	MLPPP	NTE	
	172.16.66.49	14.10	172.16.66.62	21.10	MLPPP	NTE	
	172.16.66.49	14.6	172.16.66.62	21.6	PPP	NTE	

FIGURE 16-170 NTE8 Endpoints on the Physical Map

16.14.9 Viewing NTE8 Configuration Faults

When the NTE8 configuration is set up and running, faults can be generated on four components:

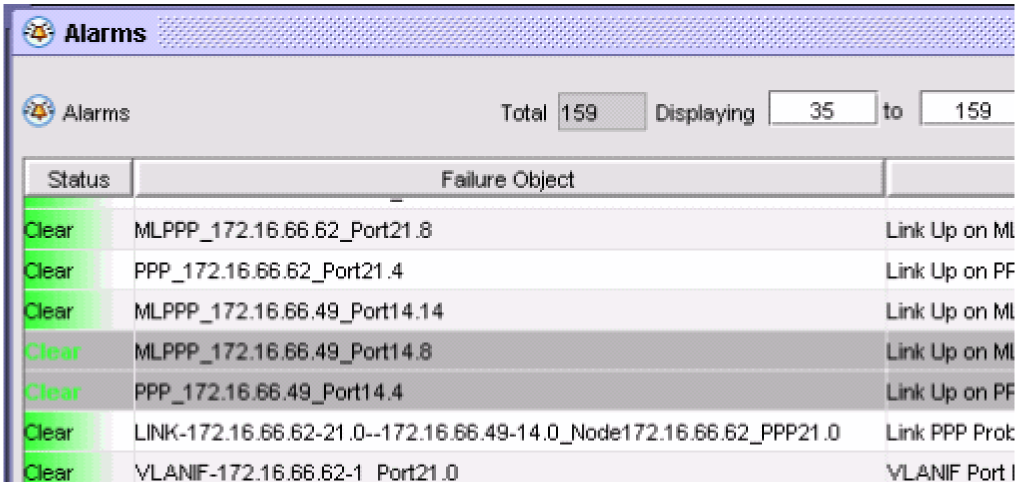
- NTE8 Card
- DS1/E1 port (such as LOS, LOF, Receiving AIS, etc.)
- PPP (Configuration Failure, Peer Disabled, etc.)
- MLPPP

Note: *Refer to the Software Reference for iMAP Series Switches for a complete description of these faults, and the Log Reference for SwitchBlade x3100 and iMAP Series Switches for a complete list of alarms.*

Trap Parsers and/or Filter are used to receive and process the iMAP PPP/MLPPP link traps into NMS Events/Alarms. (For an overview of the Fault Management system, refer to Section "Setting Up Fault Management" on page 990)

The traps are propagated as follows:

- DS1/E1 Port Alarms are generated from their corresponding Link down/up traps.
- PPP and MLPPP alarms are generated from their corresponding Link down/up traps. (Note PPPs of an MLPPP do not produce Link traps.)
- The Bandwidth Degraded alarm is generated when an interface defect trap is received from the iMAP.
- DS1/E1, PPP and MLPPP Link down/up traps are propagated to any of their associated VLANIFs and LINKs (including VLINK symbols on VLAN maps).
- MLPPP Bandwidth Degraded traps (when a PPP of an MLPPP goes down) are propagated to any of their associated VLANIFs and LINKs (including VLINK symbols on VLAN maps).



Alarms

Alarms Total 159 Displaying 35 to 159

Status	Failure Object	
Clear	MLPPP_172.16.66.62_Port21.8	Link Up on Ml
Clear	PPP_172.16.66.62_Port21.4	Link Up on PF
Clear	MLPPP_172.16.66.49_Port14.14	Link Up on Ml
Clear	MLPPP_172.16.66.49_Port14.8	Link Up on Ml
Clear	PPP_172.16.66.49_Port14.4	Link Up on PF
Clear	LINK-172.16.66.62-21.0--172.16.66.49-14.0_Node172.16.66.62_PPP21.0	Link PPP Prob
Clear	VLANIF-172.16.66.62-1 Port21.0	VLANIF Port I

FIGURE 16-171 Alarms Associated with NTE Endpoints

16.15 Upstream Control Protocol (UCP) Display

UCP is a proprietary protocol that informs other devices in the network that it is the “upstream node” for a UFO VLAN. Moreover, using UCP protocol messages, the non-upstream nodes for the UFO VLAN can dynamically determine their upstream interfaces. UCP actions occur independently of the topology feature being used; therefore, UCP can be used by itself as well as with EPSR.

Note: *For a complete explanation of UCP and how it works with various topology features, refer to the Software Reference for iMAP Series Switches.*

The NMS monitors for the UCP Node Type and Status Information. This includes:

- VLAN type (STD or Upstream)
- UCP Node Type (Primary, Secondary, Primary and Secondary, Upstream, Non-Upstream)
- UCP status (active, standby)

Node types are updated using SNMP traps from the relevant devices.

16.15.1 VLAN Submap Display

Each VLAN interface on a VLAN submap has a UCP Node-type label on top of the VLANIF symbol that can be one of the following for i MAP 6.0 devices:

- **p-ups** - Primary Upstream Node
- **s-ups** - Secondary Upstream Node
- **p&s-ups** - Primary and Secondary Upstream Node
- **non-ups** - Non-Upstream Node
- No text - the VLAN Interface is not in UFO mode; it is a standard VLAN.

Refer to the following figure. An upstream node is connected to a non-upstream node. The green color of the "p-ups" text indicates that the primary is currently active. If there were a secondary upstream node, it would be in a standby state and be indicated by a gray color.

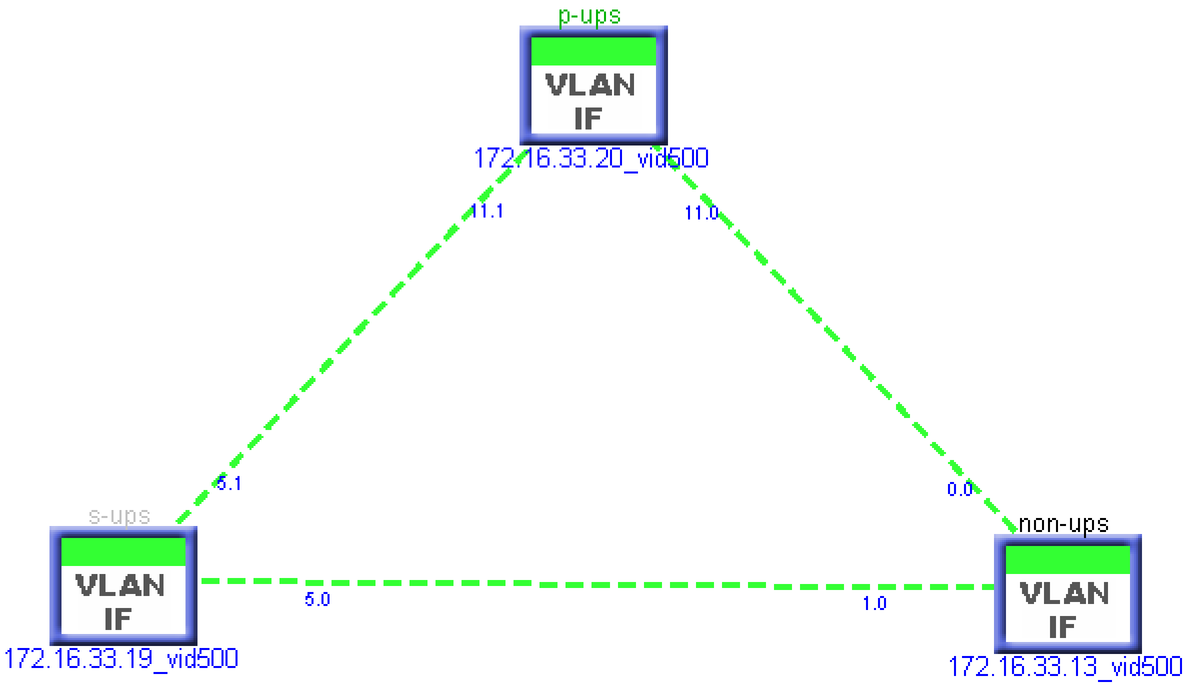
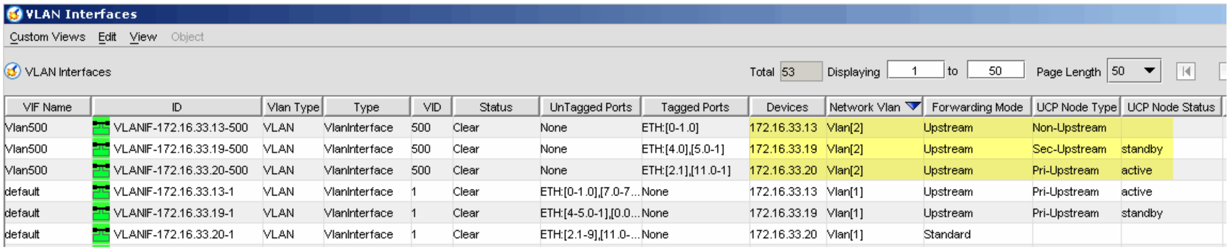


FIGURE 16-172 VLAN Interface Showing UCP Status

16.15.2 Network Inventory Display

This same information is also available in the VLAN IF inventory table. Refer to the following figure.



Total 53 Displaying 1 to 50 Page Length 50

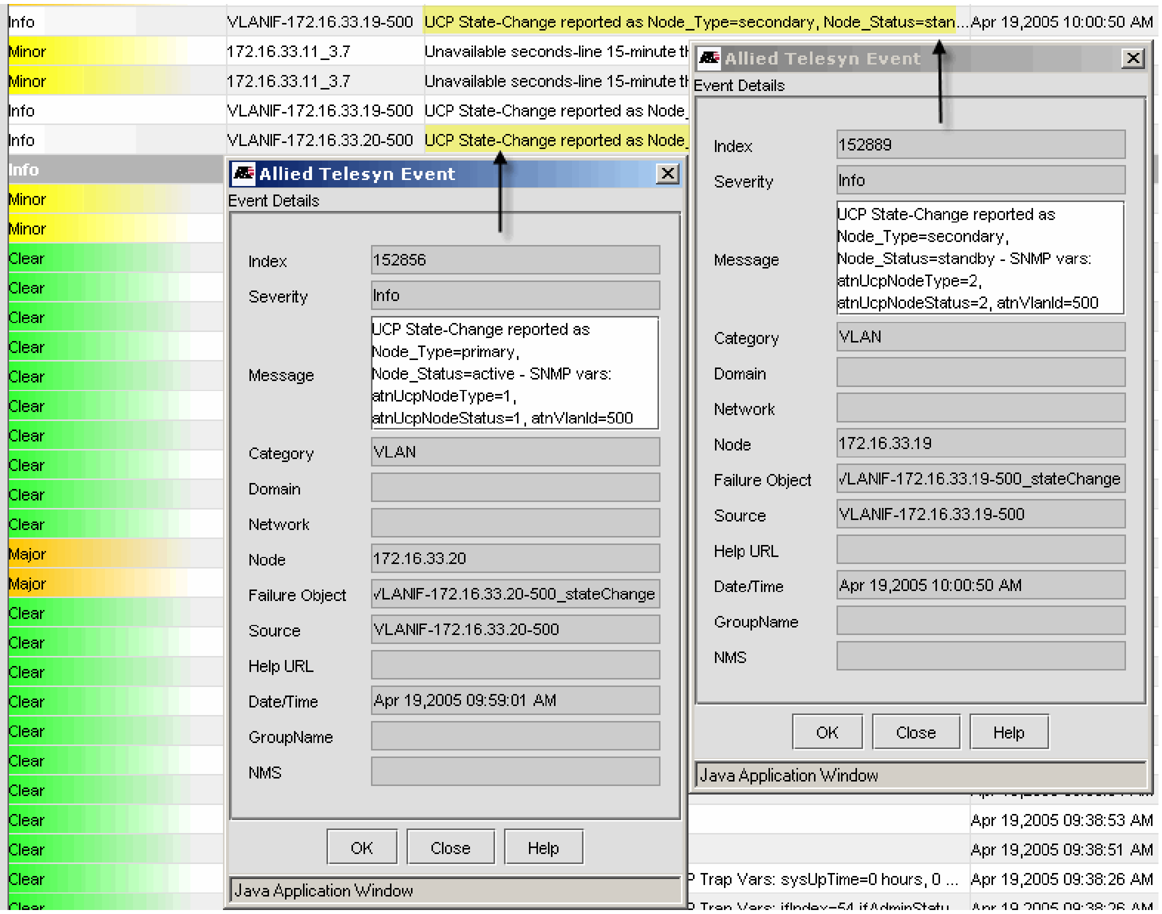
VIF Name	ID	Vlan Type	Type	VID	Status	UnTagged Ports	Tagged Ports	Devices	Network Vlan	Forwarding Mode	UCP Node Type	UCP Node Status
Vlan500	VLANIF-172.16.33.13-500	VLAN	VlanInterface	500	Clear	None	ETH:[0-1.0]	172.16.33.13	Vlan[2]	Upstream	Non-Upstream	
Vlan500	VLANIF-172.16.33.19-500	VLAN	VlanInterface	500	Clear	None	ETH:[4.0],[5.0-1]	172.16.33.19	Vlan[2]	Upstream	Sec-Upstream	standby
Vlan500	VLANIF-172.16.33.20-500	VLAN	VlanInterface	500	Clear	None	ETH:[2.1],[11.0-1]	172.16.33.20	Vlan[2]	Upstream	Pri-Upstream	active
default	VLANIF-172.16.33.13-1	VLAN	VlanInterface	1	Clear	ETH:[0-1.0],[7.0-7...	None	172.16.33.13	Vlan[1]	Upstream	Pri-Upstream	active
default	VLANIF-172.16.33.19-1	VLAN	VlanInterface	1	Clear	ETH:[4-5.0-1],[0.0...	None	172.16.33.19	Vlan[1]	Upstream	Pri-Upstream	standby
default	VLANIF-172.16.33.20-1	VLAN	VlanInterface	1	Clear	ETH:[2.1-9],[11.0-...	None	172.16.33.20	Vlan[1]	Standard		

FIGURE 16-173 UCP Status in the Network Inventory Table for the VLAN Interfaces (Highlighted)

16.15.3 Events View (Change of State)

When the active/standby status of the Primary/Secondary Node changes (because of failures in the network or administrative changes), SNMP traps are sent from the device indicating a state change. In the Events view, they appear as Info status events.

The following figures show how these changes are displayed.



Info VLANIF-172.16.33.19-500 UCP State-Change reported as Node_Type=secondary, Node_Status=stan... Apr 19,2005 10:00:50 AM
Minor 172.16.33.11_3.7 Unavailable seconds-line 15-minute th
Minor 172.16.33.11_3.7 Unavailable seconds-line 15-minute th
Info VLANIF-172.16.33.19-500 UCP State-Change reported as Node_
Info VLANIF-172.16.33.20-500 UCP State-Change reported as Node_
Info
Minor
Minor
Clear
Clear
Clear
Clear
Clear
Clear
Clear
Clear
Clear
Clear
Major
Major
Clear
Clear
Clear
Clear
Clear
Clear
Clear
Clear
Clear
Clear
Apr 19,2005 09:38:53 AM
Apr 19,2005 09:38:51 AM
P Trap Vars: sysUpTime=0 hours, 0 ... Apr 19,2005 09:38:26 AM

Index 152856
Severity Info
Message UCP State-Change reported as Node_Type=primary, Node_Status=active - SNMP vars: atnUcpNodeType=1, atnUcpNodeStatus=1, atnVlanId=500
Category VLAN
Domain
Network
Node 172.16.33.20
Failure Object VLANIF-172.16.33.20-500_stateChange
Source VLANIF-172.16.33.20-500
Help URL
Date/Time Apr 19,2005 09:59:01 AM
GroupName
NMS

Index 152889
Severity Info
Message UCP State-Change reported as Node_Type=secondary, Node_Status=standby - SNMP vars: atnUcpNodeType=2, atnUcpNodeStatus=2, atnVlanId=500
Category VLAN
Domain
Network
Node 172.16.33.19
Failure Object VLANIF-172.16.33.19-500_stateChange
Source VLANIF-172.16.33.19-500
Help URL
Date/Time Apr 19,2005 10:00:50 AM
GroupName
NMS

FIGURE 16-174 Events View when Change in UCP State (Highlighted)

Note: *Since Events are part of Alarm Management, these events can be modified going through the Events Filter and can trigger various other events/alarms. Refer to Section "Setting Up Fault Management" on page 990*

These changes are also reflected in the VLANIF submap and the VLAN Interfaces Network Inventory table.

Note: *To ensure that the status of the VLANs/interfaces is correct, the user can rediscover the relevant devices. This will appear in the Event view as a rediscovery, but if there are UCP-related changes, they will appear in the VLAN submap and Network Inventory table.*

16.16 Link Discovery

For VLAN-related features of the NMS, such as the VLAN topology maps, EPSR, and UPC features, the NMS depends on accurate link information to piece together the broadcast domain for each extended VLAN.

The LLDP protocol is a feature on devices and this provides the information needed by the AlliedView NMS to provide the GUI for Link Discovery.

This subsection describes these interfaces and the specific functions Link Discovery.

- A Physical link between iMAPs will be automatically discovered if LLDP has been activated on its link ports at each end. Note that LLDP activation **must** be done once using the CLI on each interface for which links are to be discovered.
- New links are only updated during discovery/re-discovery of the devices.
- The user can still create links manually, but when a link is discovered via LLDP and this conflicts with at least one of the ports of a manually created link, the manually created link will be deleted and the LLDP link will be added. A warning event will be sent to indicate that a link was invalid and has been deleted. The same behavior will also occur when the existing link is a previously discovered link (rather than manually created) that has been changed.

All link details, including those for discovered links, can be viewed by double-clicking on the Linkset symbol on the Physical Map, or by selecting the Physical Links table in the Network Inventory. Refer to the following figures.

Note: To configure devices so that they support LLDP, refer to "LLDP Protocol and Associated Features (LAG/VCS Monitoring)" on page 313.

16.17 Software Upgrade with EPSR

16.17.1 Overview

Section "Standard Load Software Configuration" on page 298 explains the software download application and how it can be used to control the download process for one or more devices and prevent errors.

A special situation occurs when the devices are part of an EPSR configuration, because the order in which the devices are downloaded will prevent service outage. Following are the rules/constraints that must be followed to ensure nodes in an EPSR configuration are upgraded without loss of service:

- Whenever a set of nodes is selected to be upgraded, if any of the nodes contain EPS Rings, it is possible that additional nodes, not specified in the original set, will have to be upgraded before the specified nodes.
- Any additional node of an EPSR may then have other EPSRs on it that require additional nodes to be upgraded before others.
- If any EPSR in the chain of EPSRs is misconfigured then it may not be possible to derive the upgrade order of its nodes. (The preferred order is: Master, Secondary Transit, around to Primary Transit.) It is possible that another valid EPSR will require a node from this invalid EPSR to be upgraded before the valid one can be upgraded.
- The upgrade of one node should be complete before the upgrade of another node is begun.
- If an EPSR is only partially managed, so that the topology is linear from Master to Secondary Transit, but not a complete ring back to the Primary Transit, then the partial ring should still be upgraded (under the assumption that any unmanaged remaining Transit nodes of the ring will be upgraded subsequently, either via CLI or another management system).
- Even when all EPSRs are valid there may still be loops in the precedence order (e.g., two EPSRs on the same ports, going in opposite directions will result in precedence loops.) Loops in the precedence order indicate that there is no order of upgrade among the nodes that will satisfy all EPSR's constraints. In this case, the user will have to modify or ignore certain EPSR vlans to form an upgradeable set of ring configurations.

In release 9.0, the download application is enhanced so that when a device is selected for download, the EPSR configuration is checked so that these rules are followed:

- If the devices chosen are part of an EPSR configuration, and there are no conflicts with the configuration rules listed above, the devices are upgraded in the proper order, and so service is not disrupted.
- If there is an ambiguity or conflict in the EPSR configuration, GUIs appear informing that the AlliedView NMS needs to resolve these conflicts before proceeding.
- If the selected device set does not include those that are part of the EPSR configuration, GUIs appear informing that the AlliedView NMS needs to include these devices before proceeding.
- If the EPSR has not been configured correctly initially, the feature cannot work, and a GUI with the appropriate error message appears; the user can choose to upgrade anyway if a potential loss of service is either acceptable or data traffic is not running over the VLANs.

Note: The Software Configuration feature is included in Section 5, since it can perform actions on a specific device. However, since this feature checks multiple devices it is considered a network service.

16.17.2 Upgrading all Nodes for an EPSR Ring

Following is an example that shows how the feature works when upgrading multiple devices that include an EPSR Control and Data VLAN The administrator wishes to upgrade the three devices that make an EPSR ring, as shown in the following figures.

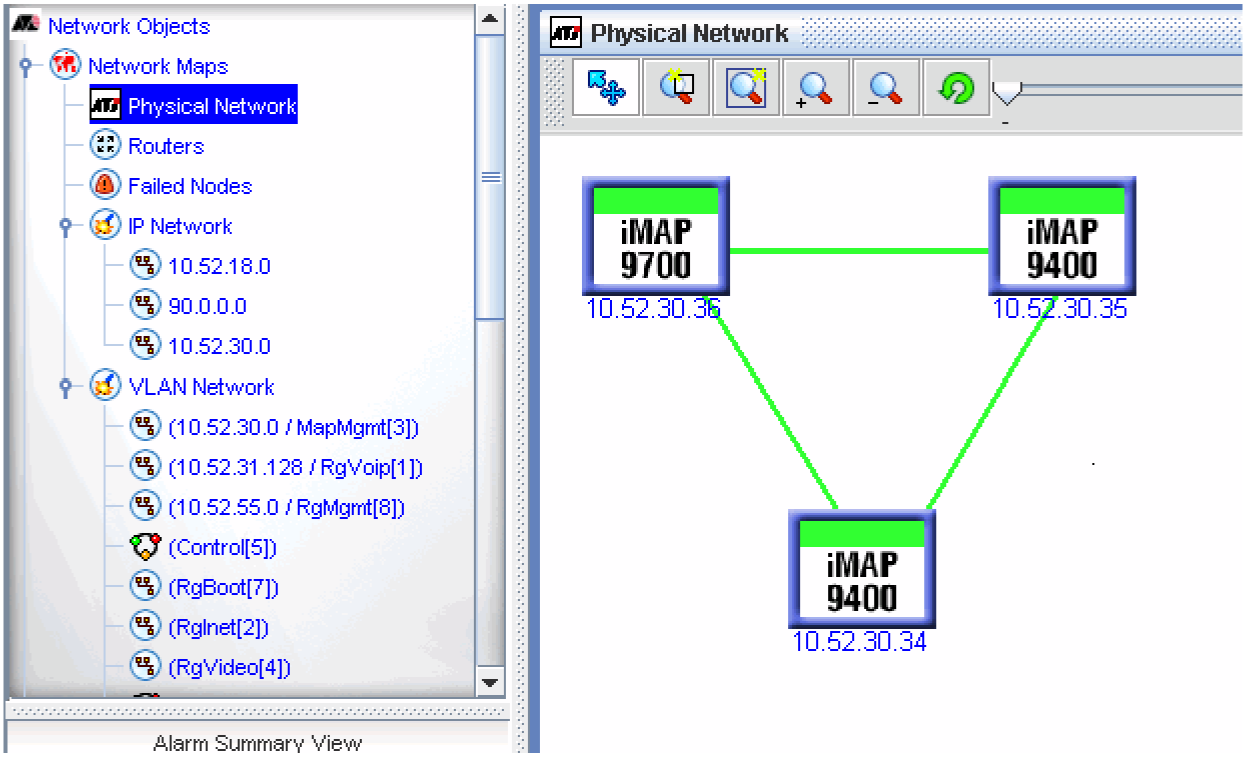


FIGURE 16-175 Physical Map showing Ring Configuration

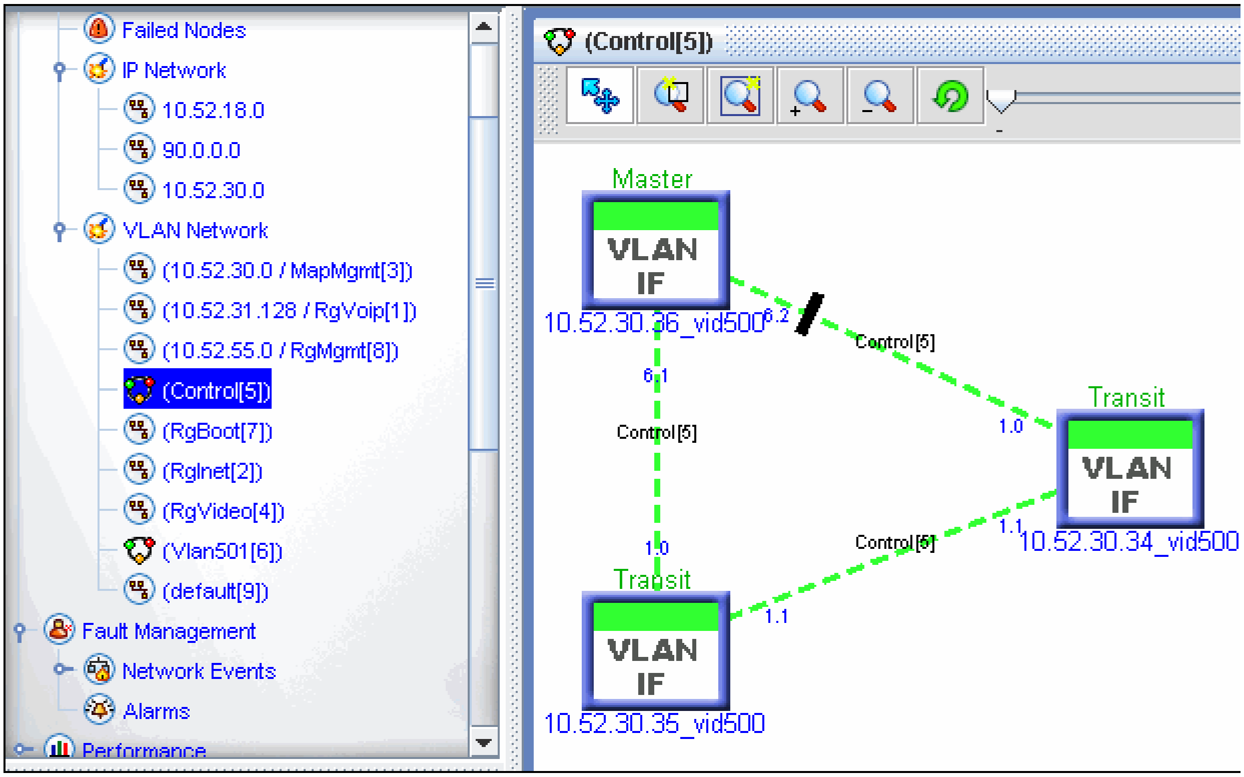


FIGURE 16-176 EPSR - Control VLAN over Physical Links

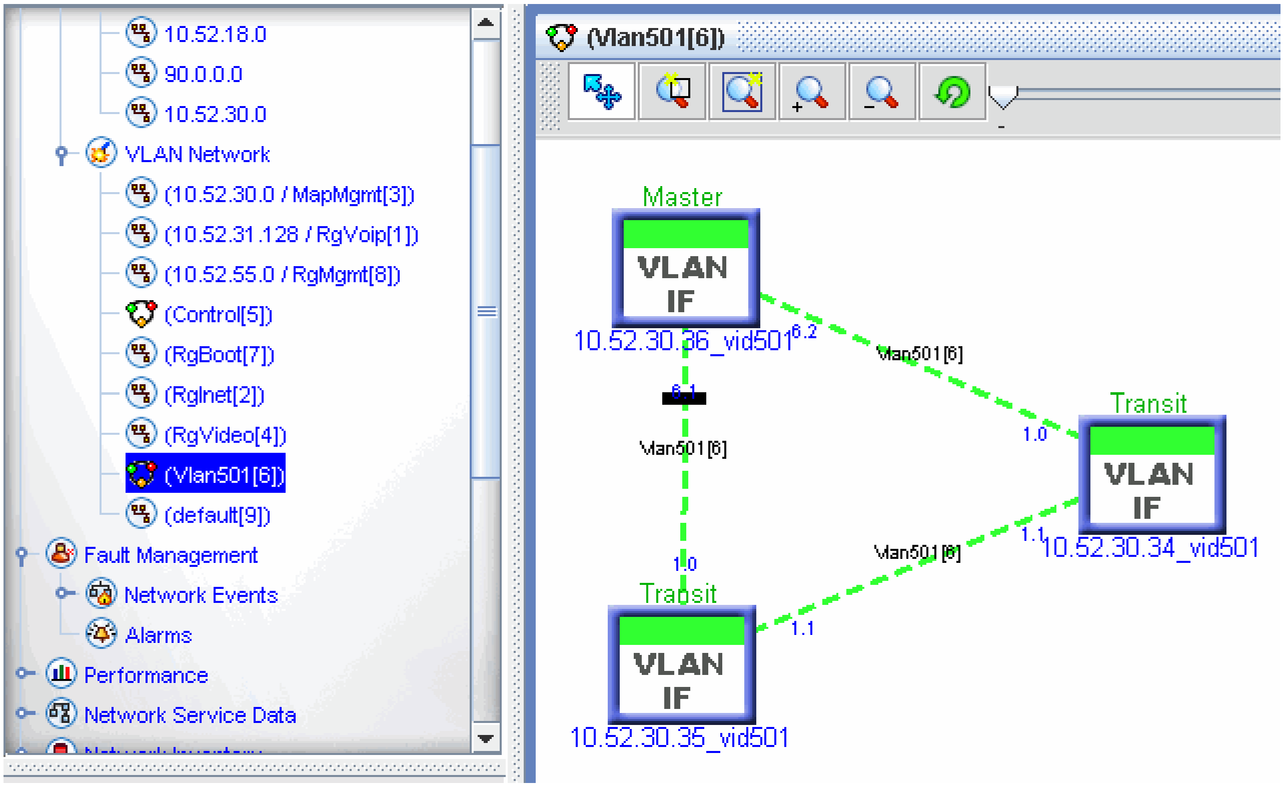
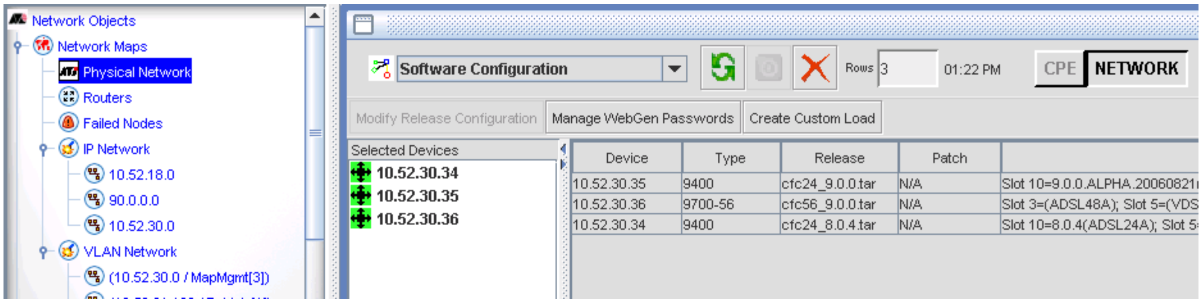


FIGURE 16-177 EPSR - Data VLAN over Physical Links

In the physical map, the user could highlight the three devices, right click and select Software Configuration. This would bring up the Software configuration with all three devices included, as shown below.

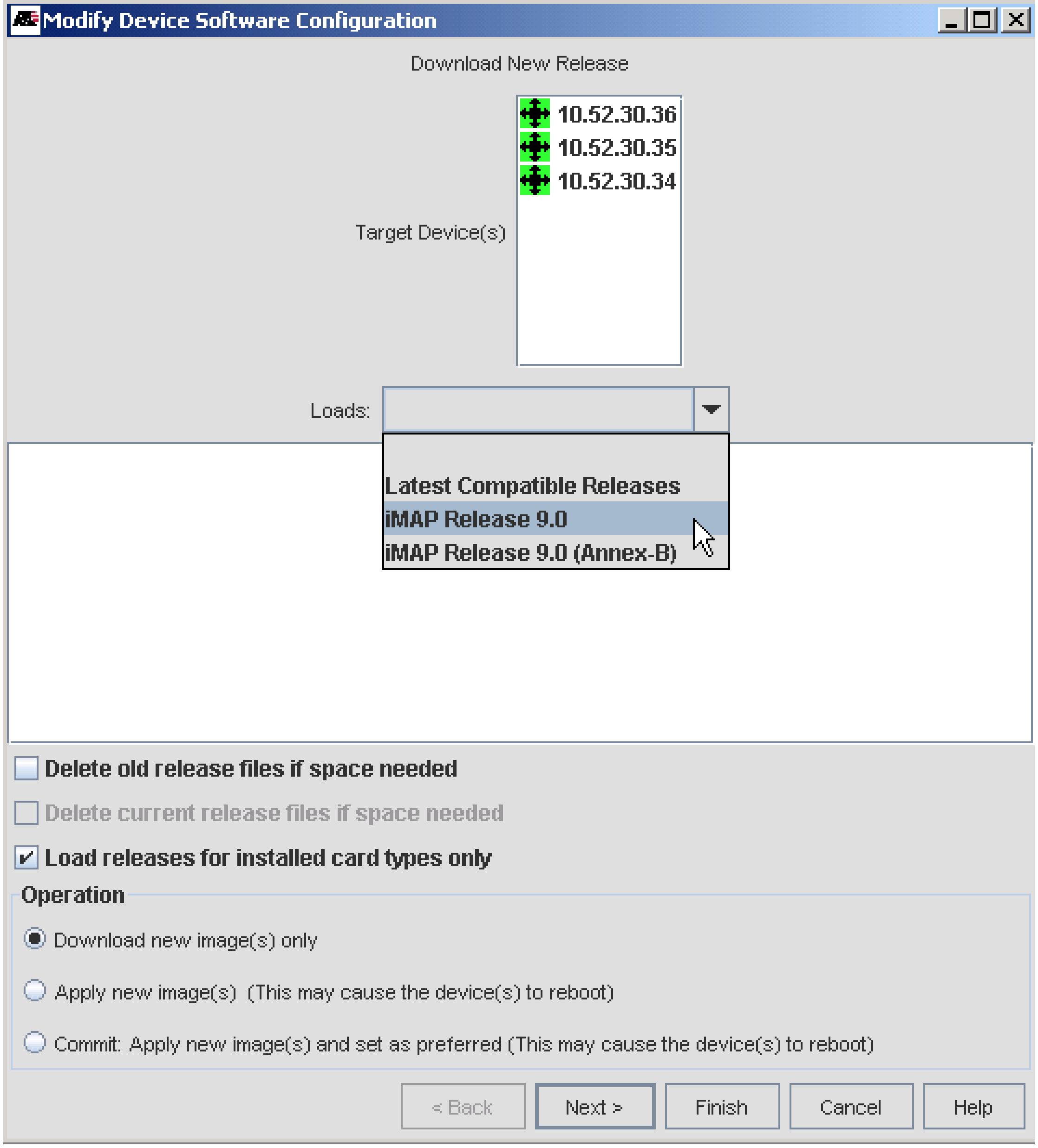


Selected Devices
10.52.30.34
10.52.30.35
10.52.30.36

Device	Type	Release	Patch	
10.52.30.35	9400	cfc24_9.0.0.tar	N/A	Slot 10=9.0.0.ALPHA.20060821
10.52.30.36	9700-56	cfc56_9.0.0.tar	N/A	Slot 3=(ADSL48A); Slot 5=(VDS
10.52.30.34	9400	cfc24_8.0.4.tar	N/A	Slot 10=8.0.4(ADSL24A); Slot 5

FIGURE 16-178 Devices Chosen for Software Upgrade

The user would select all three devices and click on the now active **Modify Release Configuration** button. This would bring up the Modify Device Software Configuration window, as shown in the following figure and explained in "Standard Load Software Configuration" on page 298.



Modify Device Software Configuration

Download New Release

Target Device(s)

10.52.30.36
10.52.30.35
10.52.30.34

Loads:

Latest Compatible Releases
iMAP Release 9.0
iMAP Release 9.0 (Annex-B)

☐ Delete old release files if space needed

☐ Delete current release files if space needed

☑ Load releases for installed card types only

Operation

● Download new image(s) only

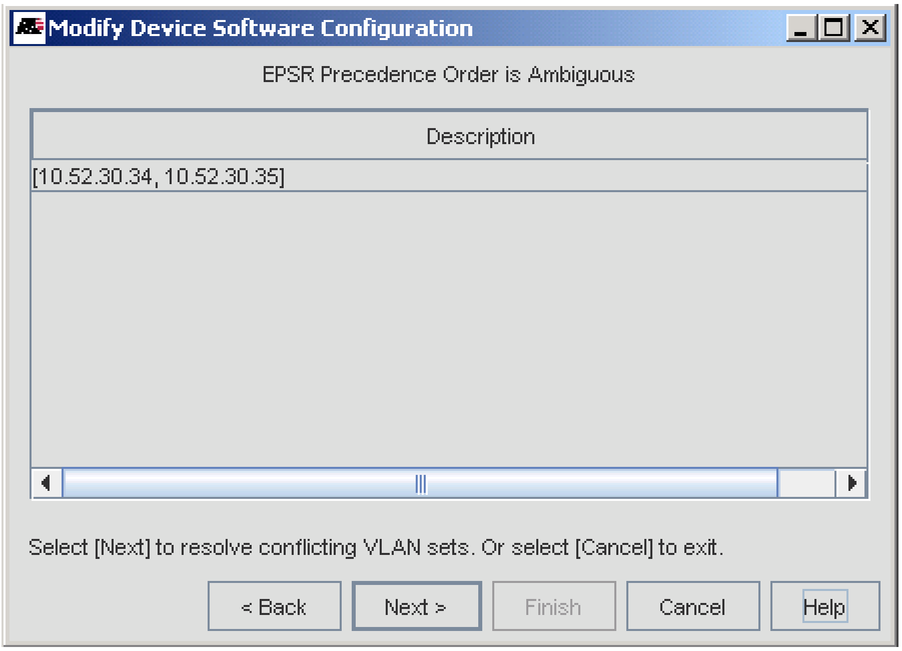
○ Apply new image(s) (This may cause the device(s) to reboot)

○ Commit: Apply new image(s) and set as preferred (This may cause the device(s) to reboot)

FIGURE 16-179 Modify Device Software Configuration Window - Select Load for Multiple Devices

When the user selects Next, the AlliedView NMS checks the EPSR configuration and, using the configuration rules listed above, determines the order in which the devices should be loaded. In this example, as the user clicks **Next**, the following screens appear, as shown in the following figures:

- EPSR Precedence Order is Ambiguous - If the user selects Next, the AlliedView NMS determines which of the two nodes to upgrade first.
- Remove Conflicting EPSR Loops - If the user selects Next, the AlliedView NMS determines which VLAN to ignore.



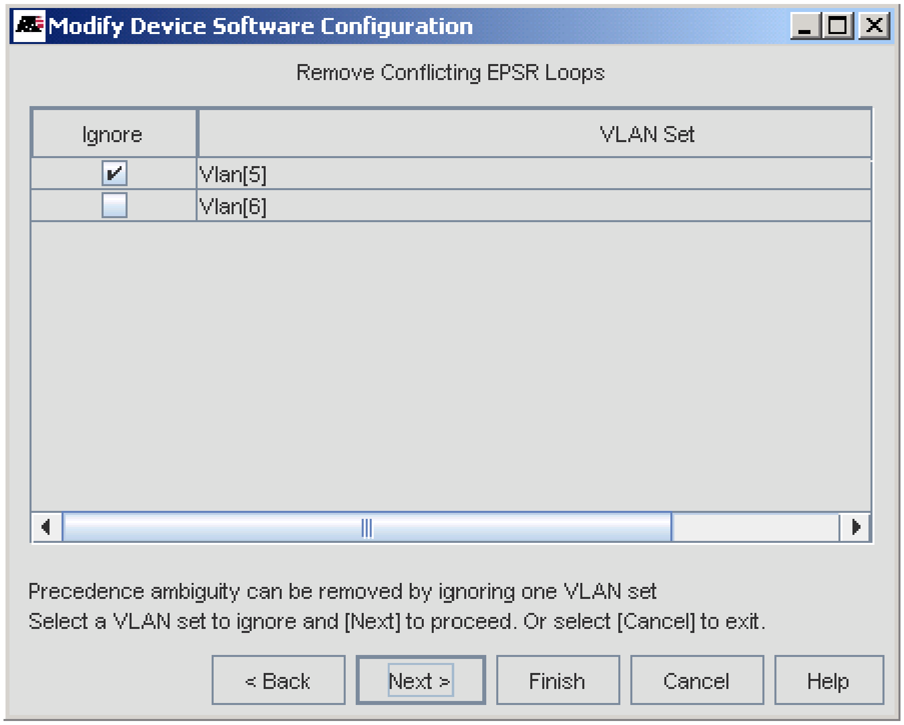
Modify Device Software Configuration

EPSR Precedence Order is Ambiguous

Description
[10.52.30.34, 10.52.30.35]

Select [Next] to resolve conflicting VLAN sets. Or select [Cancel] to exit.

FIGURE 16-180 Resolving Conflicting VLAN Sets



Modify Device Software Configuration

Remove Conflicting EPSR Loops

Ignore	VLAN Set
☑	Vlan[5]
□	Vlan[6]

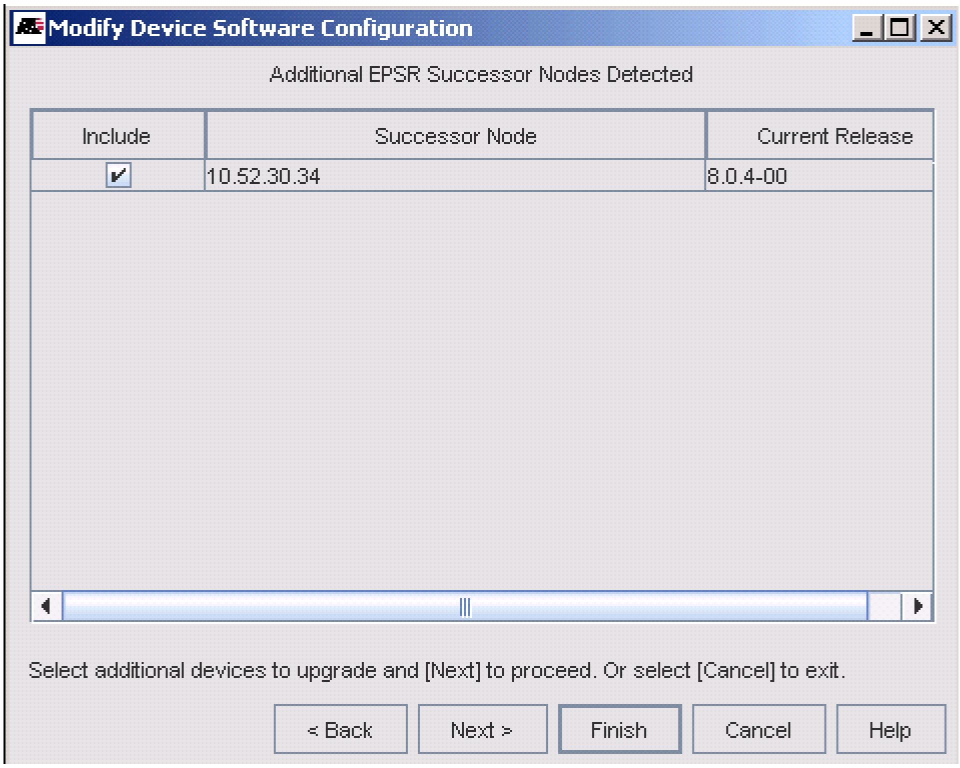
Precedence ambiguity can be removed by ignoring one VLAN set
Select a VLAN set to ignore and [Next] to proceed. Or select [Cancel] to exit.

FIGURE 16-181 Selecting a VLAN to ignore during Upgrade

16.17.3 Upgrading One Node that is part of an EPSR Configuration

In the previous example, the EPSR configuration included three devices, and all three devices were selected for a software upgrade. If the user does not choose all the devices that take part in the EPSR configuration, the AlliedView NMS determines that additional devices must be upgraded as well. Two other GUIs may therefore appear while performing the upgrade sequence:

- Additional EPSR Successor Nodes Detected - A successor node must be included in the upgrade procedure. The user should ensure all the listed devices are checked and select Next.
- Additional EPSR Predecessor Nodes Detected - A predecessor node must be included in the upgrade procedure. The user should ensure all the listed devices are checked and select Next.

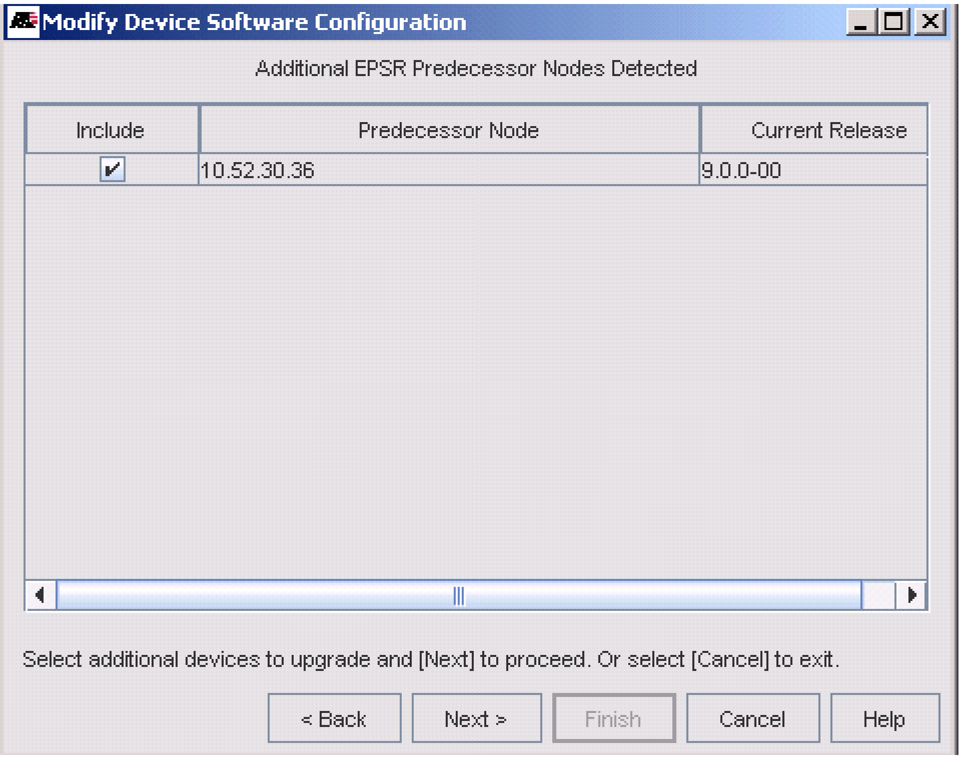


Additional EPSR Successor Nodes Detected

Include	Successor Node	Current Release
☑	10.52.30.34	8.0.4-00

Select additional devices to upgrade and [Next] to proceed. Or select [Cancel] to exit.

FIGURE 16-182 Select Additional Successor Devices to Upgrade



Additional EPSR Predecessor Nodes Detected

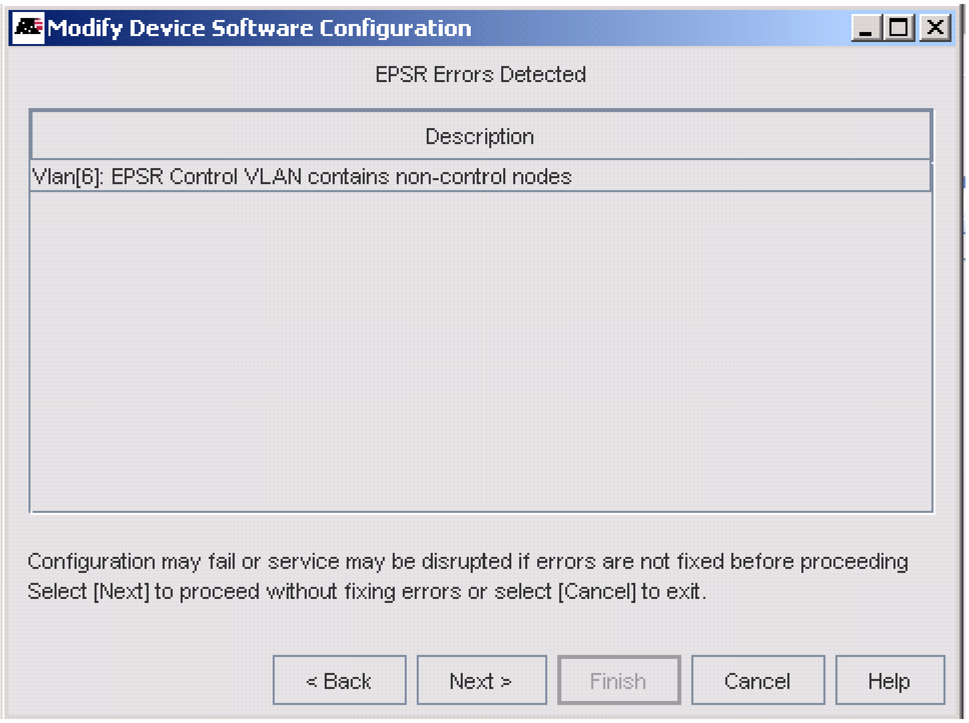
Include	Predecessor Node	Current Release
☑	10.52.30.36	9.0.0-00

Select additional devices to upgrade and [Next] to proceed. Or select [Cancel] to exit.

FIGURE 16-183 Select Additional Predecessor Devices to Upgrade

16.17.4 Upgrading Devices when EPSR not Properly Configured

If EPSR has been improperly configured and the user selects one or more devices to upgrade, a GUI with an error message appears that warns the user that if the error is not fixed the configuration will fail or data service may be disrupted. Refer to the following figure.



EPSR Errors Detected

Description
Vlan[6]: EPSR Control VLAN contains non-control nodes

Configuration may fail or service may be disrupted if errors are not fixed before proceeding
Select [Next] to proceed without fixing errors or select [Cancel] to exit.

FIGURE 16-184 Error Condition for Upgrade

16.18 Diagnostic Audit

The NMS provides the capability to run diagnostic audits on certain network entities. Currently, the entities that can be audited are:

- Network VLANs
- CES Circuits

Audits are started from the “Diagnostic Audit Reporting” window, which can be launched from various menus within the NMS. The appropriate Audit Entity IDs will appear in the window, based on the menu from which it was launched.

Running an audit will check the configuration of the Audit Entity to determine potential problems with that entity’s configuration, and generate a report detailing those identified problems. The problems are categorized as follows:

- Errors - These are problems in the configuration that are incorrect and can cause the failure of features.
- Warnings - These are for potential problems that may not be what the user intended
- Informational - These generally include parameters collected from the audit that provide the user with a snapshot of the current configuration.

16.18.1 Network VLANs

The sample Diagnostic Audit screen below was launched from the background menu on the VLAN Map associated with Network VLAN ID “Vlan[52]”. In this example, only the Errors and Warnings categories have been selected for the report.

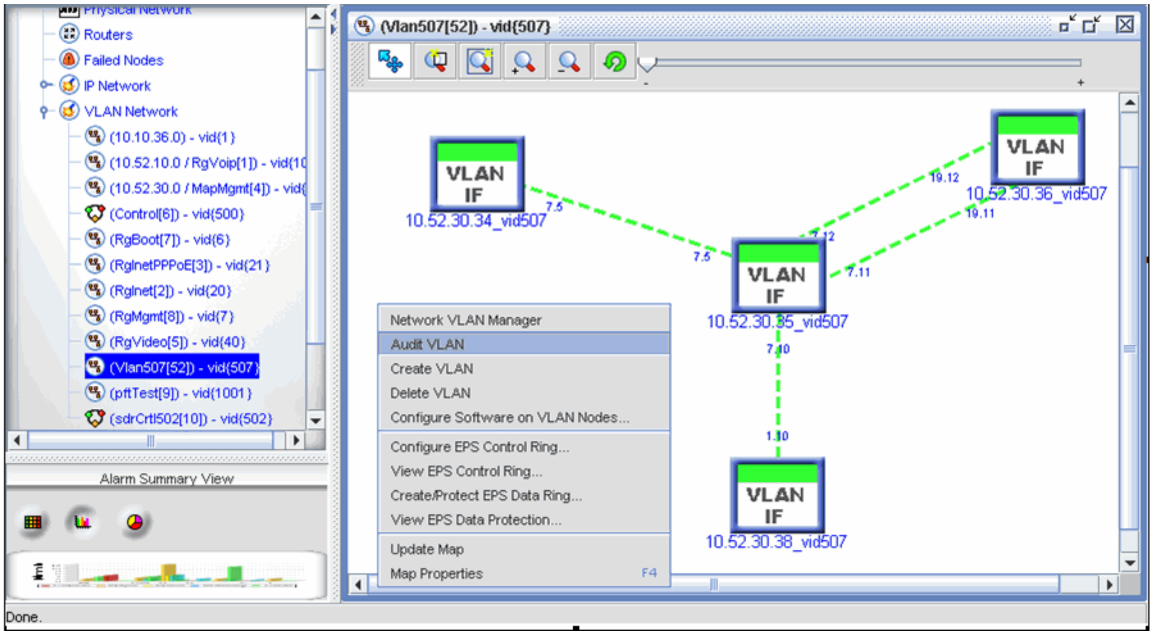
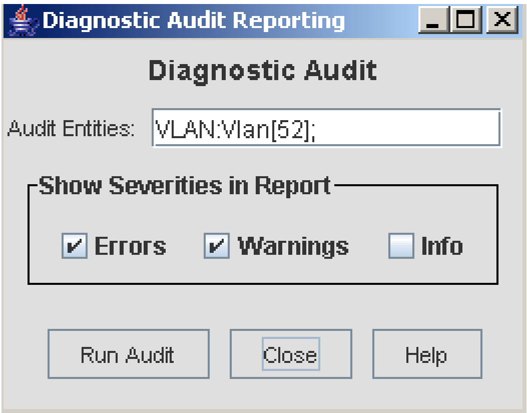


FIGURE 16-185 Audit Selection for Network VLAN

Selecting the Audit VLAN menu item brings up the Diagnostic Audit screen with the selected VLAN, as shown in the following figure.


Diagnostic Audit Reporting

Diagnostic Audit

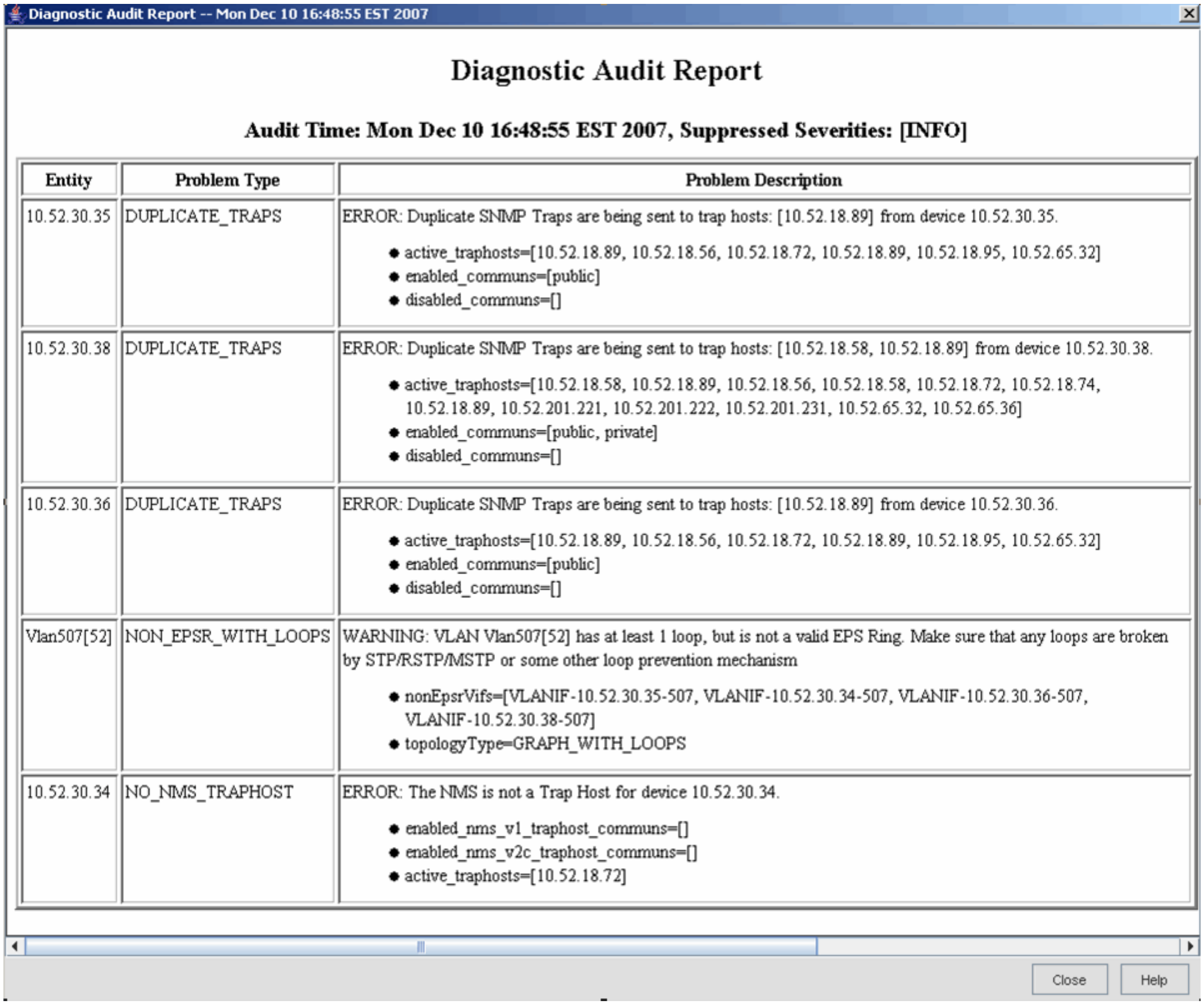
Audit Entities: VLAN:Vlan[52];

Show Severities in Report

☑ Errors ☑ Warnings □ Info

FIGURE 16-186 Diagnostic Audit Panel

The Run Audit button starts the audit and resulted in the following audit report.



Diagnostic Audit Report

Audit Time: Mon Dec 10 16:48:55 EST 2007, Suppressed Severities: [INFO]

Entity	Problem Type	Problem Description
10.52.30.35	DUPLICATE_TRAPS	ERROR: Duplicate SNMP Traps are being sent to trap hosts: [10.52.18.89] from device 10.52.30.35. ● active_traphosts=[10.52.18.89, 10.52.18.56, 10.52.18.72, 10.52.18.89, 10.52.18.95, 10.52.65.32] ● enabled_communs=[public] ● disabled_communs=[]
10.52.30.38	DUPLICATE_TRAPS	ERROR: Duplicate SNMP Traps are being sent to trap hosts: [10.52.18.58, 10.52.18.89] from device 10.52.30.38. ● active_traphosts=[10.52.18.58, 10.52.18.89, 10.52.18.56, 10.52.18.58, 10.52.18.72, 10.52.18.74, 10.52.18.89, 10.52.201.221, 10.52.201.222, 10.52.201.231, 10.52.65.32, 10.52.65.36] ● enabled_communs=[public, private] ● disabled_communs=[]
10.52.30.36	DUPLICATE_TRAPS	ERROR: Duplicate SNMP Traps are being sent to trap hosts: [10.52.18.89] from device 10.52.30.36. ● active_traphosts=[10.52.18.89, 10.52.18.56, 10.52.18.72, 10.52.18.89, 10.52.18.95, 10.52.65.32] ● enabled_communs=[public] ● disabled_communs=[]
Vlan507[52]	NON_EPSR_WITH_LOOPS	WARNING: VLAN Vlan507[52] has at least 1 loop, but is not a valid EPS Ring. Make sure that any loops are broken by STP/RSTP/MSTP or some other loop prevention mechanism ● nonEpsrVifs=[VLANIF-10.52.30.35-507, VLANIF-10.52.30.34-507, VLANIF-10.52.30.36-507, VLANIF-10.52.30.38-507] ● topologyType=GRAPH_WITH_LOOPS
10.52.30.34	NO_NMS_TRAPHOST	ERROR: The NMS is not a Trap Host for device 10.52.30.34. ● enabled_nms_v1_traphost_communs=[] ● enabled_nms_v2c_traphost_communs=[] ● active_traphosts=[10.52.18.72]

FIGURE 16-187 Example Audit Report

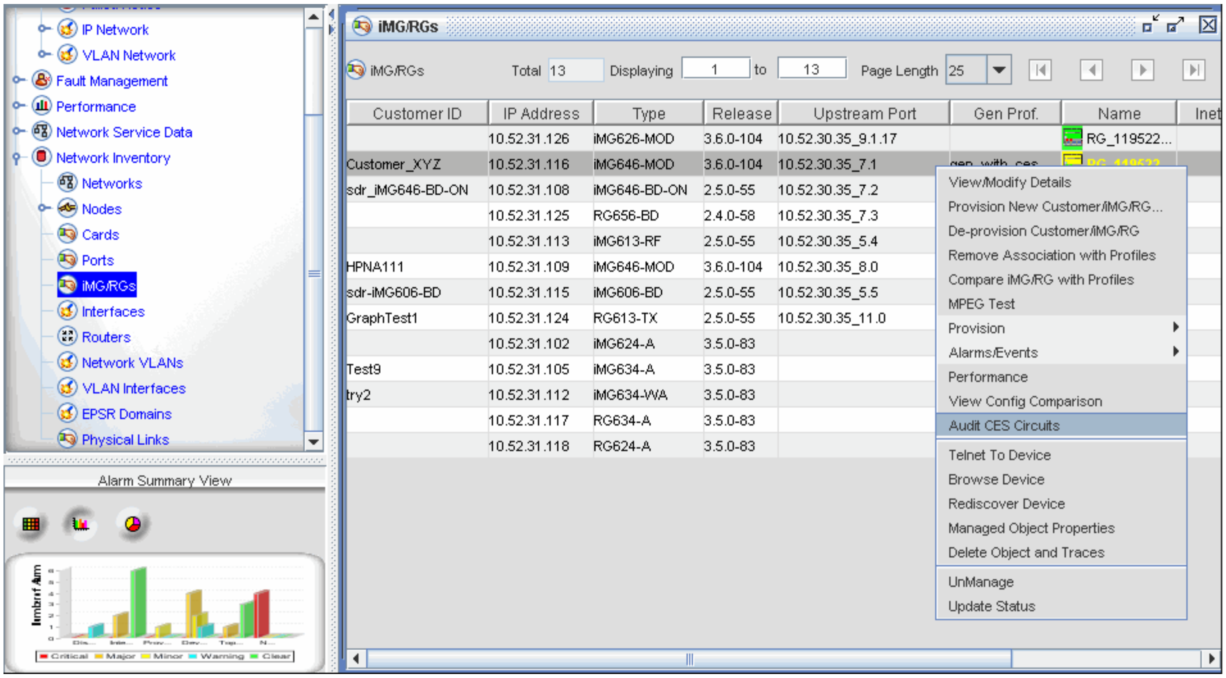
16.18.2 Audit the CES Circuit on the iMG6x6MOD or CES8 Card

A similar audit capability is provided for CES Circuits. These entities can be launched from the following locations:

- Port Table – Audits the CES circuit on each selected port from the Port Table in the Network Inventory (can select multiple ports from the table)
- iMG/RG Table – Audits the CES circuits on each selected iMG from the iMG/RG Table in the Network Inventory (can select multiple iMGs from the table)
- Card Table – Audits the CES circuits on each selected card from the Card Table in the Network Inventory (can select multiple cards from the table)
- Node Table – Audits the CES circuits on each selected device from the Node Table in the Network Inventory (can select multiple devices from the table)
- Physical Network Map – Audits the CES circuits on each selected device from the Physical Network Map, by right-clicking on the device icon and going to the Network Service sub-menu (can select multiple devices from the map)

A CES Audit will check for configuration problems at both ends of the circuit, if the peer port is also managed by the NMS.

The following figure shows how an audit can be initiated from the pull-down menu in the iMG/RG table.

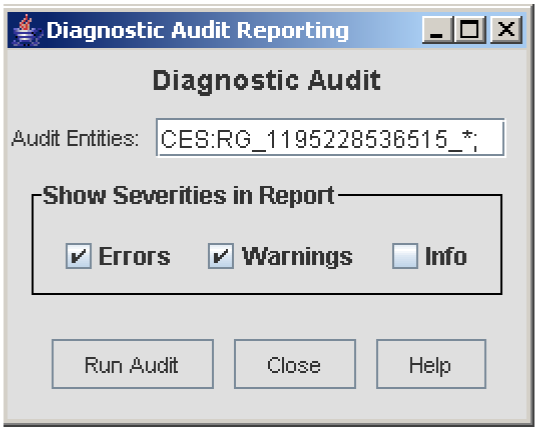


iMG/RGs Total 13 Displaying 1 to 13 Page Length 25

Customer ID	IP Address	Type	Release	Upstream Port	Gen Prof.	Name	Inet
	10.52.31.126	iMG626-MOD	3.6.0-104	10.52.30.35_9.1.17		RG_119522...	
Customer_XYZ	10.52.31.116	iMG646-MOD	3.6.0-104	10.52.30.35_7.1	gen_with_ces	RG_119522	
sdr_iMG646-BD-ON	10.52.31.108	iMG646-BD-ON	2.5.0-55	10.52.30.35_7.2			
	10.52.31.125	RG656-BD	2.4.0-58	10.52.30.35_7.3			
	10.52.31.113	iMG613-RF	2.5.0-55	10.52.30.35_5.4			
HPNA111	10.52.31.109	iMG646-MOD	3.6.0-104	10.52.30.35_8.0			
sdr-iMG606-BD	10.52.31.115	iMG606-BD	2.5.0-55	10.52.30.35_5.5			
GraphTest1	10.52.31.124	RG613-TX	2.5.0-55	10.52.30.35_11.0			
	10.52.31.102	iMG624-A	3.5.0-83				
Test9	10.52.31.105	iMG634-A	3.5.0-83				
try2	10.52.31.112	iMG634-WA	3.5.0-83				
	10.52.31.117	RG634-A	3.5.0-83				
	10.52.31.118	RG624-A	3.5.0-83				

FIGURE 16-188 Accessing the Audit CES Circuit Panel for iMG6x6MOD

After selecting the **Audit CES Circuits** in the pull-down, the Diagnostic Audit panel appears, as shown in the following figure.



Diagnostic Audit Reporting

Diagnostic Audit

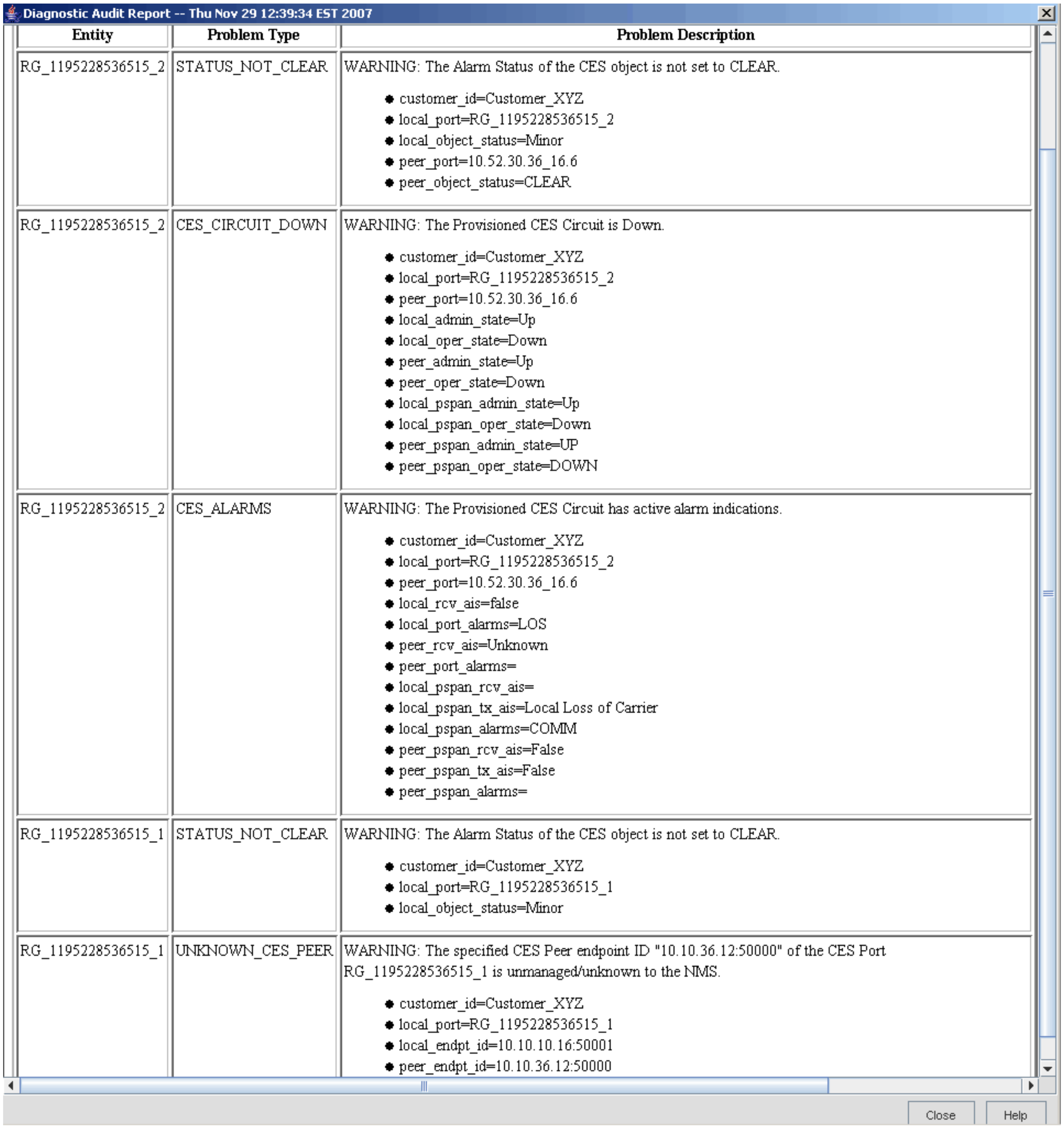
Audit Entities: CES:RG_1195228536515_*;

Show Severities in Report

☑ Errors ☑ Warnings □ Info

FIGURE 16-189 CES Circuit Audit Panel

The Run Audit button starts the audit and results in the following audit report.



Diagnostic Audit Report -- Thu Nov 29 12:39:34 EST 2007

Entity	Problem Type	Problem Description
RG_1195228536515_2	STATUS_NOT_CLEAR	WARNING: The Alarm Status of the CES object is not set to CLEAR. ● customer_id=Customer_XYZ ● local_port=RG_1195228536515_2 ● local_object_status=Minor ● peer_port=10.52.30.36_16.6 ● peer_object_status=CLEAR
RG_1195228536515_2	CES_CIRCUIT_DOWN	WARNING: The Provisioned CES Circuit is Down. ● customer_id=Customer_XYZ ● local_port=RG_1195228536515_2 ● peer_port=10.52.30.36_16.6 ● local_admin_state=Up ● local_oper_state=Down ● peer_admin_state=Up ● peer_oper_state=Down ● local_pspan_admin_state=Up ● local_pspan_oper_state=Down ● peer_pspan_admin_state=UP ● peer_pspan_oper_state=DOWN
RG_1195228536515_2	CES_ALARMS	WARNING: The Provisioned CES Circuit has active alarm indications. ● customer_id=Customer_XYZ ● local_port=RG_1195228536515_2 ● peer_port=10.52.30.36_16.6 ● local_rcv_ais=false ● local_port_alarms=LOS ● peer_rcv_ais=Unknown ● peer_port_alarms= ● local_pspan_rcv_ais= ● local_pspan_tx_ais=Local Loss of Carrier ● local_pspan_alarms=COMM ● peer_pspan_rcv_ais=False ● peer_pspan_tx_ais=False ● peer_pspan_alarms=
RG_1195228536515_1	STATUS_NOT_CLEAR	WARNING: The Alarm Status of the CES object is not set to CLEAR. ● customer_id=Customer_XYZ ● local_port=RG_1195228536515_1 ● local_object_status=Minor
RG_1195228536515_1	UNKNOWN_CES_PEER	WARNING: The specified CES Peer endpoint ID "10.10.36.12:50000" of the CES Port RG_1195228536515_1 is unmanaged/unknown to the NMS. ● customer_id=Customer_XYZ ● local_port=RG_1195228536515_1 ● local_endpt_id=10.10.10.16:50001 ● peer_endpt_id=10.10.36.12:50000

FIGURE 16-190 Results of Running CES Audit

16.19 Port Authentication (802.1x)

The main components of Port Authentication are:

- The Authenticator - the port on the SBx3100 that wishes to enforce authentication before allowing access to services that are accessible behind it. The SBx3100 plays this role.
- The Supplicant -the user device attached to the Authenticator that wishes to access services offered by the authenticator's system. The supplicant may be a PC or other device connected to the Authenticator either directly or via a hub
- The Authentication Server (RADIUS) - a device that uses the authentication credentials supplied by the supplicant (using 802.1X method described below), via the authenticator, or from the authenticator itself (using MAC based authentication method) to determine if the authenticator should grant access to the network. Once authorized, the Authentication server notifies the Authenticator to allow access. The Authentication Server may also supply other information pertaining to the supplicant such as a particular VLAN to use.

Port authentication can be implemented with the following methods:

- 802.1X - This uses the IEEE Standard 802.1X standard. The supplicant is required to use 802.1X and supply the authentication credentials to the Authentication Server via the Authenticator.
- MAC-based authentication - This uses the source MAC address of the supplicant for authentication. When the Authenticator receives the frame from a newly learned source MAC, the Authenticator generates a RADIUS request for authentication.
- Web-based authentication - A username/password pair is entered from the client’s browser. When the switch receives the pair, it generates a RADIUS request for authentication.

The Authenticator can be configured to authorize one supplicant or more than one supplicant, as follows:

- Single Host - Only one (single) supplicant that is authorized can be allowed to communicate on the Authenticator port. The other supplicant is disallowed.
- Multi Host - More than one supplicant is possible on the Authenticator port. When any one supplicant succeeds with authentication, the other supplicants are automatically considered to be authenticated and can communicate on the port. This mode is known as 'Piggyback Mode' also.
- Multi Supplicant - More than one supplicant is possible on the Authenticator port. However each supplicant has to be individually authenticated. Some supplicants are allowed and some supplicants may be disallowed when a supplicant failed to authenticate.

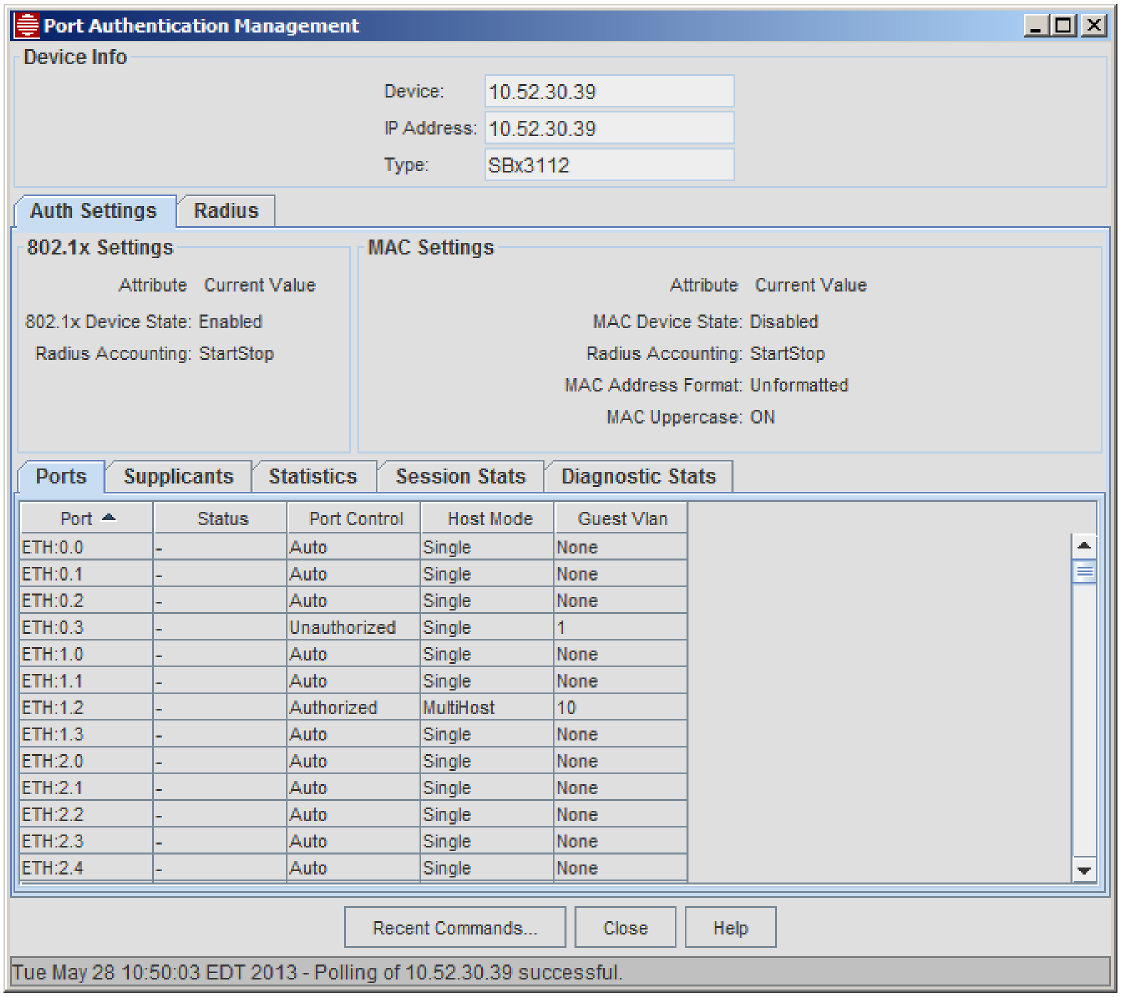
The NMS supports the following:

- 802.1x method
- MAC Authentication method
- Single Host, Multi Host, and Multi Supplicant

Note: Configuring RADIUS is not part of the NMS provisioning, and must be done separately.

16.19.1 Port Authentication for a Device

1. To access port authentication management, do one of the following in the **Network Objects** panel:
   - Go to **Network Maps** > **Physical Network**. In the **Physical Network** screen, select the device.
   - Go to **Network Inventory** > **Nodes**. In the **Nodes** screen, select the device.
2. Go to **Operations** > **Port Authentication Management**. The **Port Authentication Management** screen appears.



Device Info

Device: 10.52.30.39

IP Address: 10.52.30.39

Type: SBx3112

802.1x Settings

Attribute	Current Value
802.1x Device State:	Enabled
Radius Accounting:	StartStop

MAC Settings

Attribute	Current Value
MAC Device State:	Disabled
Radius Accounting:	StartStop
MAC Address Format:	Unformatted
MAC Uppercase:	ON

Port ▲	Status	Port Control	Host Mode	Guest Vlan
ETH:0.0	-	Auto	Single	None
ETH:0.1	-	Auto	Single	None
ETH:0.2	-	Auto	Single	None
ETH:0.3	-	Unauthorized	Single	1
ETH:1.0	-	Auto	Single	None
ETH:1.1	-	Auto	Single	None
ETH:1.2	-	Authorized	MultiHost	10
ETH:1.3	-	Auto	Single	None
ETH:2.0	-	Auto	Single	None
ETH:2.1	-	Auto	Single	None
ETH:2.2	-	Auto	Single	None
ETH:2.3	-	Auto	Single	None
ETH:2.4	-	Auto	Single	None

Tue May 28 10:50:03 EDT 2013 - Polling of 10.52.30.39 successful.

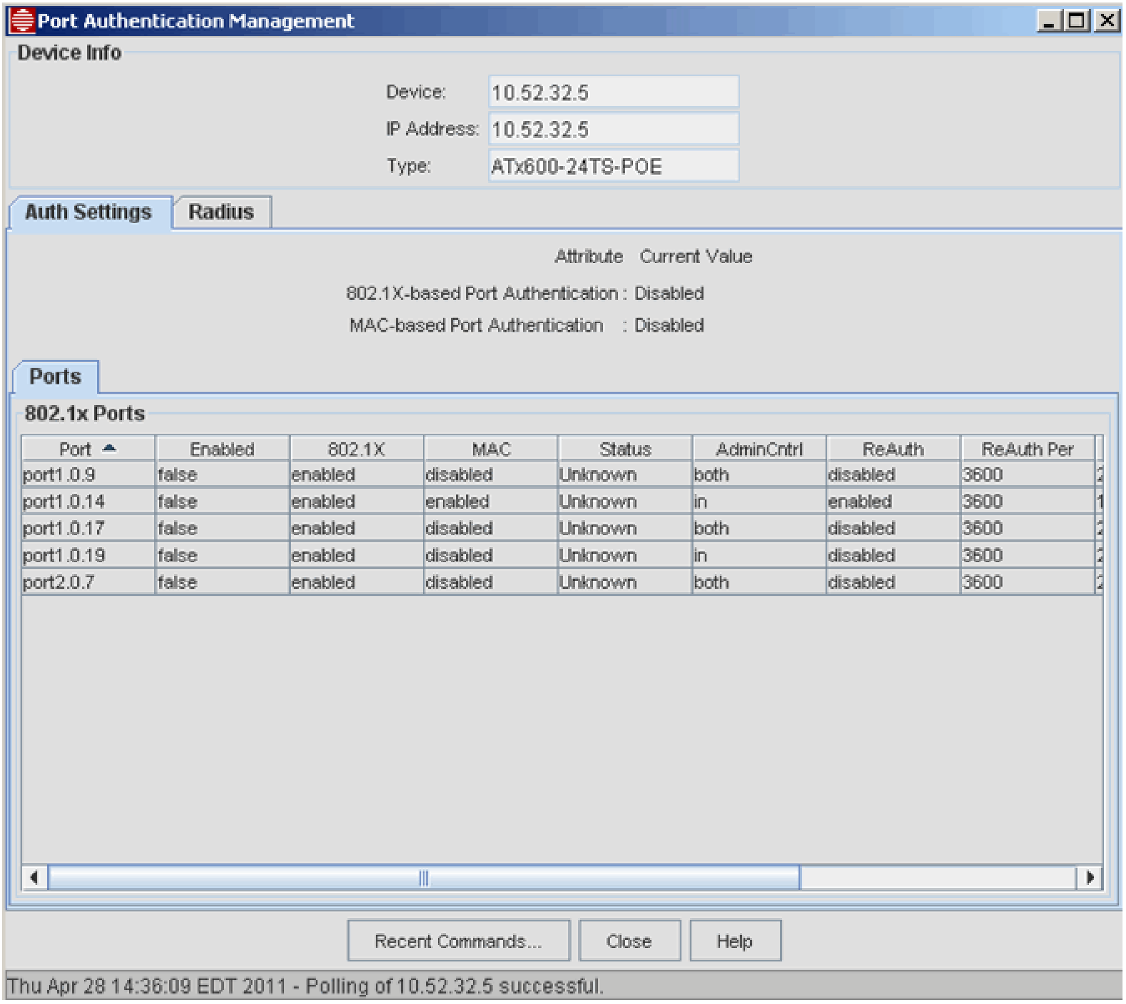
FIGURE 16-191 Port Authentication Management - SBx3100 Device

The screen contains two tabs, **Auth Settings** and **Radius**. The **Auth Settings** tab has the following subtabs:

- Ports - The status of Port Authentication (Enabled or Disabled), Port Control, Host Mode, and Guest Vlan.
- Supplicants - The attributes of supplicants that have successfully connected.
- Statistics - For each port the MAC address and counts of 802.1X protocol frames.
- Session Stats - For each port the MAC address and attributes for a completed session.
- Diagnostic Stats

The Radius Tab allows the user to view the RADIUS attributes that have been configured.

For the AlliedwarePlus devices the Port Authentication Management window, there are some differences in the display regarding what data for each port is displayed. Refer to the following figure.



Device Info

Device: 10.52.32.5
IP Address: 10.52.32.5
Type: ATx600-24TS-POE

Attribute Current Value
802.1X-based Port Authentication : Disabled
MAC-based Port Authentication : Disabled

802.1x Ports

Port	Enabled	802.1X	MAC	Status	AdminCntrl	ReAuth	ReAuth Per	
port1.0.9	false	enabled	disabled	Unknown	both	disabled	3600	2
port1.0.14	false	enabled	enabled	Unknown	in	enabled	3600	1
port1.0.17	false	enabled	disabled	Unknown	both	disabled	3600	2
port1.0.19	false	enabled	disabled	Unknown	in	disabled	3600	2
port2.0.7	false	enabled	disabled	Unknown	both	disabled	3600	2

Thu Apr 28 14:36:09 EDT 2011 - Polling of 10.52.32.5 successful.

FIGURE 16-192 Port Authentication Configuration - AlliedWare Plus Device

16.19.2 Profiles with the Port Authentication Feature

To configure Port Authentication for a port, the Profiles can be used so that the feature is automatically enabled when the port is brought into service. The following Profiles include Port Authentication.

Note: Although the feature can be changed on the Service Management window for the port, it is recommended to use Profiles and the Triple-Play form to configure the feature, since this will lead to fewer errors when configuring a large number of ports.

16.19.2.1 SBx3100 and AlliedWare Plus Device Profiles

The following figure shows the menu to bring up a profile for an iMAP (SBx3100) and AlliedWare Plus devices.

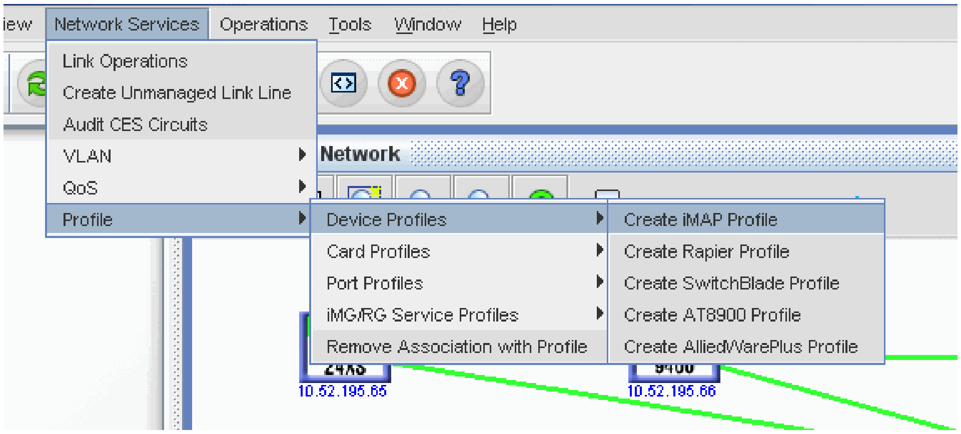
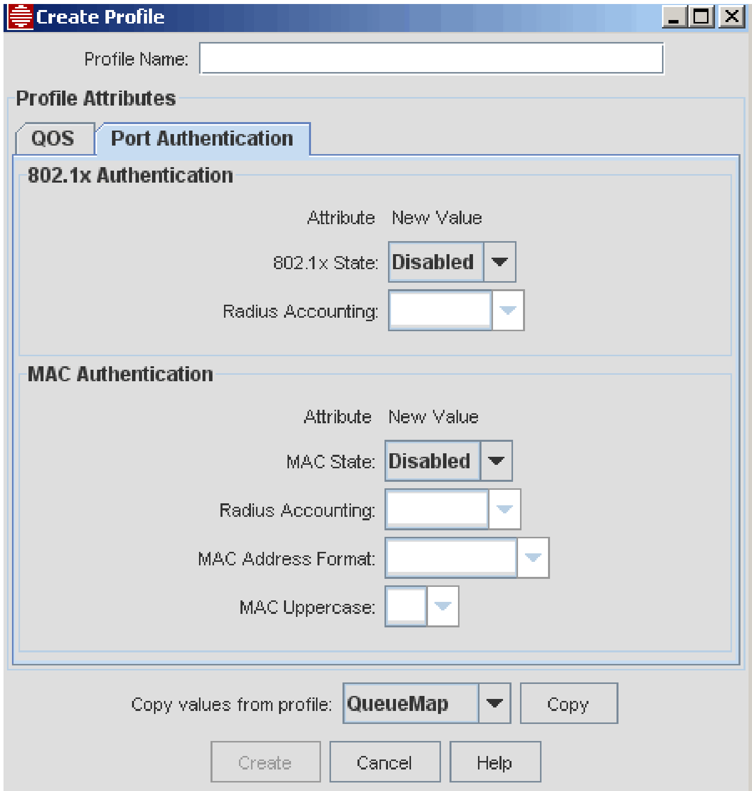


FIGURE 16-193 Profile for Port Authentication for SBx3100

The Profile itself has a Port Authentication tab, with options for 802.1x and MAC Authentication. For AlliedWare Plus devices, there is the added field Radius Group, when a set of Radius servers are combined with a group label. (If there is not a group, the label “Radius” is filled in.). Refer to the following figure.


Create Profile

Profile Name:

Profile Attributes

QOS | Port Authentication

802.1x Authentication

Attribute New Value

802.1x State: Disabled

Radius Accounting:

MAC Authentication

Attribute New Value

MAC State: Disabled

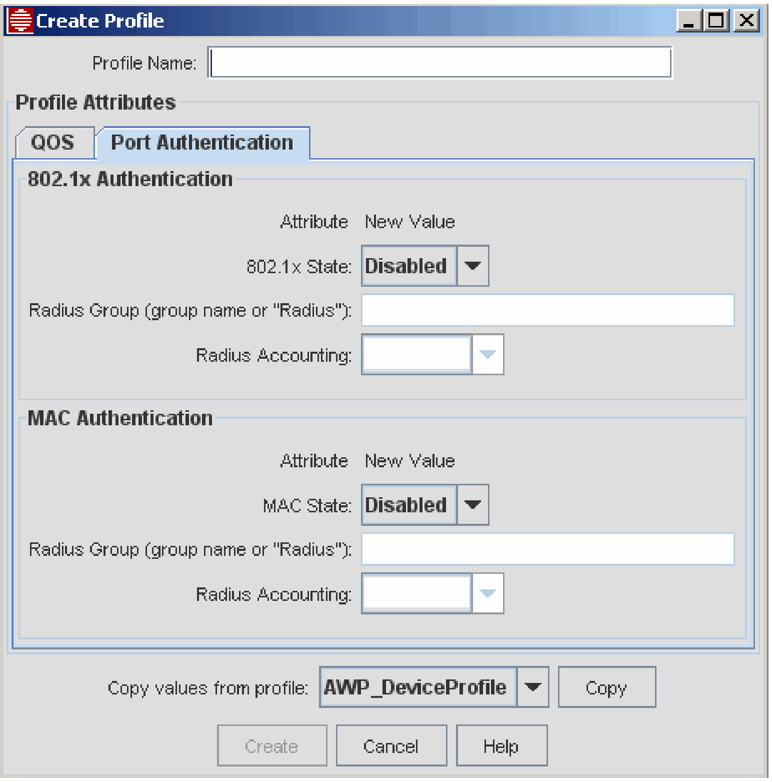
Radius Accounting:

MAC Address Format:

MAC Uppercase:

Copy values from profile: QueueMap

FIGURE 16-194 Profile for Port Authentication - SBx3100 (Includes MAC Authentication)



Profile Name:

802.1x Authentication

Attribute	New Value
802.1x State:	Disabled
Radius Group (group name or "Radius"):	
Radius Accounting:	

MAC Authentication

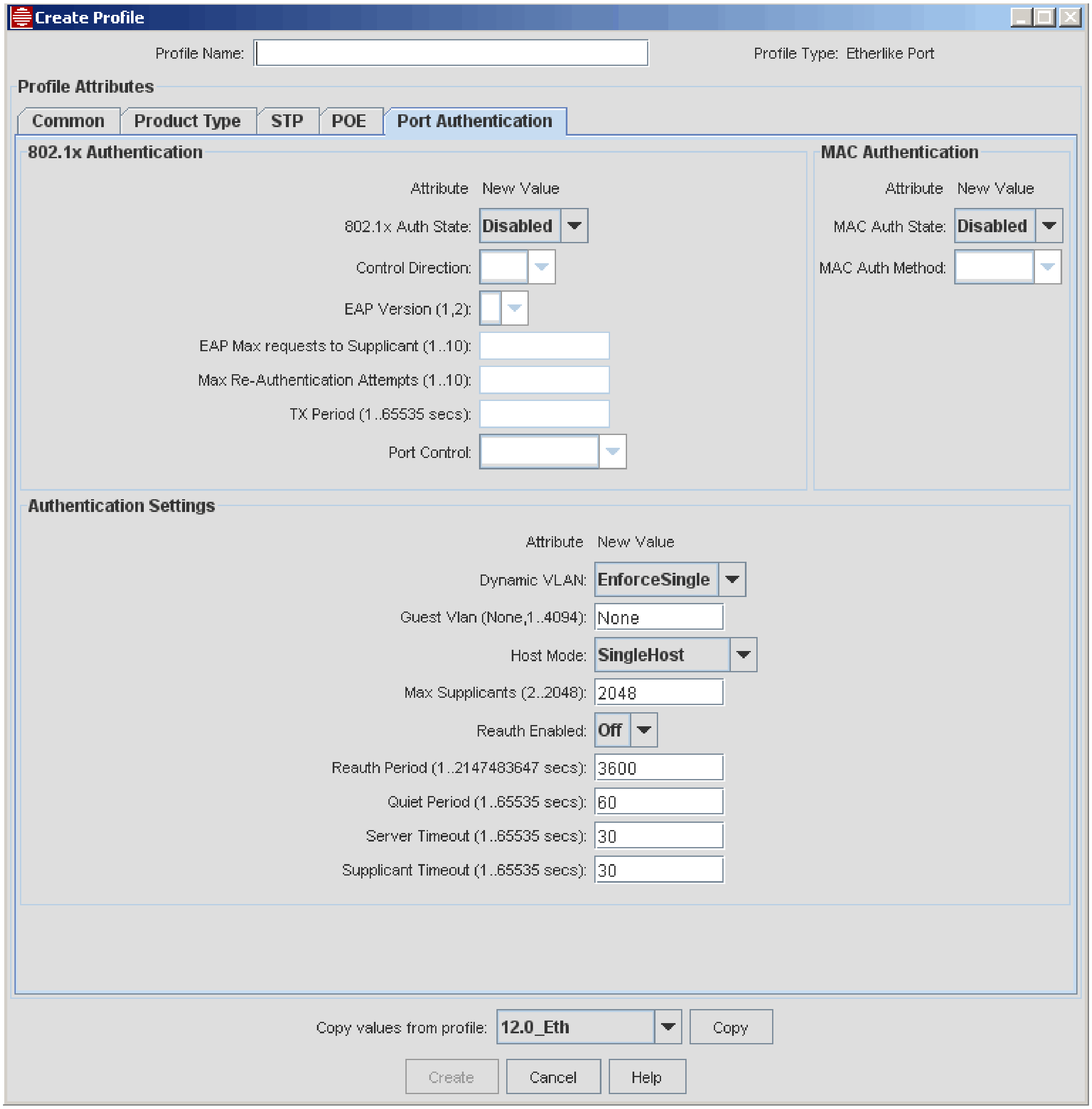
Attribute	New Value
MAC State:	Disabled
Radius Group (group name or "Radius"):	
Radius Accounting:	

Copy values from profile: AWP_DeviceProfile

FIGURE 16-195 Profile for Port Authentication - AlliedWare Plus Devices (Includes MAC Authentication)

16.19.3 Etherlike Port Profile

With this Profile the Port Authentication tab is used, and it provides the attributes needed to activate Port Authentication. (Refer to device specific documents, such as the *Software Reference for SwitchBlade x3100 Series*, for details on these fields.) Refer to the following figure. Note that there is a panel for MAC-based authentication and that the common Port Authentication settings are grouped that apply to both 802.1x and MAC-based.



Profile Name:

Profile Type: Etherlike Port

Profile Attributes

802.1x Authentication

Attribute	New Value
802.1x Auth State:	Disabled
Control Direction:	
EAP Version (1,2):	
EAP Max requests to Supplicant (1..10):	
Max Re-Authentication Attempts (1..10):	
TX Period (1..65535 secs):	
Port Control:	

MAC Authentication

Attribute	New Value
MAC Auth State:	Disabled
MAC Auth Method:	

Authentication Settings

Attribute	New Value
Dynamic VLAN:	EnforceSingle
Guest Vlan (None,1..4094):	None
Host Mode:	SingleHost
Max Supplicants (2..2048):	2048
Reauth Enabled:	Off
Reauth Period (1..2147483647 secs):	3600
Quiet Period (1..65535 secs):	60
Server Timeout (1..65535 secs):	30
Supplicant Timeout (1..65535 secs):	30

Copy values from profile: 12.0_Eth

FIGURE 16-196 Profile for Etherlike Port - Port Authentication

16.19.4 Feature Support (AlliedWare Plus and iMAP Devices)

Although much of the functionality is the same between the SBx3100 and the AlliedWare Plus of Port Authentication, there are some settings for the AlliedWare Plus devices that are not included in the configuration settings, as follows:

- Auth-fail – set auth-fail vlan
- Critical – operation in case there is no response from radius server
- Log – configure log message outputs
- Roaming – to be able to move supplicant to other port not re-authentication

- Supplicant Mac – enable port auth specified MAC address
- Keytransmit – transmit 802.1x authentication key

These items are not in the profiles nor in the view/modify screen, as explained below.

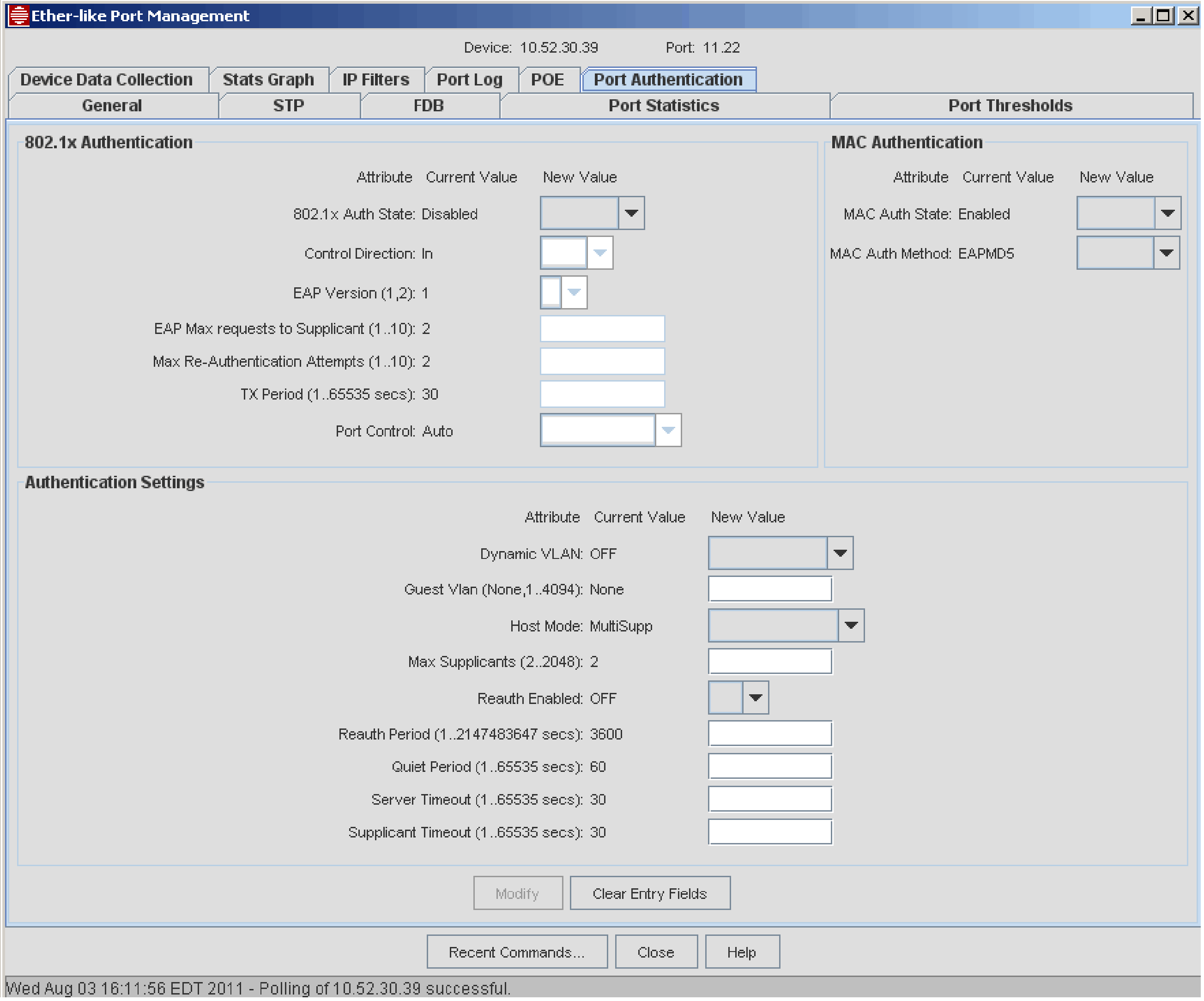
For settings that are common between the AlliedWare Plus devices and iMAP devices (the SBx3100), there are some differences in the settings, as listed below.

TABLE 16-9 Port Authorization Parameter Values - SBx3100 and AlliedWare Plus

Parameter	SBx3100 Values	AlliedWare Plus Values	Notes
Dynamic Vlan	None Single EnforceSingle	None Single Multi	Each choice is shown to the user in the profile but it will fail if the wrong setting is sent to that device. In the view modify screen the selection is limited to only the values valid for that device type.
Reauth Period	2147483647 secs	4294967295 secs	The range presented in the profile is the smaller of the two (SBx3100 value). This is also limited in the view/ modify. The smaller range is already in years.
Max Supplicants	2…2048	2…1024	The range presented in the profile is the larger of the two. If the range applied to the AWP is above the max then it defaults to the max allowable (1024). In the view modify the correct range is enforced.
Various attributes with “enable/disable” instead of “on/ off”			These are set and shown in the client as on/off even though enable or disable is sent in the background.

16.19.5 Implementing Port Authentication with Triple-Play

When Port Authentication for the device is enabled and the Etherlike Port Form is set so 802.1X or MAC-based is enabled, the user can fill out the Triple-Play form and include the Etherlike Port Profile. When the port is placed in service, Port Authentication is enabled, as shown in the Service Management window.



Device: 10.52.30.39 Port: 11.22

802.1x Authentication

Attribute	Current Value	New Value
802.1x Auth State:	Disabled	
Control Direction:	In	
EAP Version (1,2):	1	
EAP Max requests to Supplicant (1..10):	2	
Max Re-Authentication Attempts (1..10):	2	
TX Period (1..65535 secs):	30	
Port Control:	Auto	

MAC Authentication

Attribute	Current Value	New Value
MAC Auth State:	Enabled	
MAC Auth Method:	EAPMD5	

Authentication Settings

Attribute	Current Value	New Value
Dynamic VLAN:	OFF	
Guest Vlan (None,1..4094):	None	
Host Mode:	MultiSupp	
Max Supplicants (2..2048):	2	
Reauth Enabled:	OFF	
Reauth Period (1..2147483647 secs):	3600	
Quiet Period (1..65535 secs):	60	
Server Timeout (1..65535 secs):	30	
Supplicant Timeout (1..65535 secs):	30	

Wed Aug 03 16:11:56 EDT 2011 - Polling of 10.52.30.39 successful.

FIGURE 16-197 Service Management Form - Port Authentication Active

Note: *Once Port Authentication is enabled (by setting to Enabled at both device and port), you cannot add or delete a VLAN on that port. The following type of error is seen in the console window when modifying a VLAN on a port (via view/modify the port or deploy/apply the port profile):*

```
delete VLAN=40 interface=1.2
Processing.....
 Error (040626) Port Authentication has been enabled on ETH: [1.2]
officer SEC>>
```

To add or delete a VLAN, you must disable Port Authorization (either disable the feature on the port or deprovision the port).

Note: *For the SBx3100, you cannot have both 802.1x and MAC Authentication enabled on the same port. Refer to the Software Reference for SwitchBlade x3100 Series for more information.*

17. Configuring Anonymous FTP

The NMS requires an anonymous FTP server if you are managing Genband or iMG devices. This section describes how to install an FTP server for the NMS.

17.1 Windows

To install an FTP server on Windows, you must install and configure Internet Information Services (IIS), the web server software included with Windows. To install IIS, follow the documentation included with your Windows platform.

17.2 Linux

The NMS has been tested with the vsftpd FTP server on the Linux platform.

17.2.1 Installing the FTP Server

To install the vsftpd FTP server:

1. Create the FTP root directory on your system. In the sample configuration file provided with the NMS, the root directory is:

   ```
   /opt/ftp
   ```

   The directory you create must match the value of the **anon_root** parameter in the configuration file.

2. Run the following command:

   ```
   yum install vsftpd
   ```

The vsftpd FTP server is installed.

17.2.2 Sample Configuration File

A sample configuration file for the vsftpd FTP server is located at **/etc/vsftpd/vsftpd.conf**. For anonymous FTP, replace the contents of the file with the sample content displayed below.

```
#
# Allied Telesis FTP Configuration
#
listen=YES
local_enable=YES
anonymous_enable=YES
write_enable=YES
anon_root=/opt/ftp
anon_upload_enable=YES
anon_mkdir_write_enable=YES
#
# Optional directives
#
```

```
anon_max_rate=2048000
xferlog_enable=YES
# listen_address=10.52.18.230
listen_port=21
chown_uploads=YES
chown_username=ftp
ftp_username=ftp
log_ftp_protocol=YES
anon_umask=0022
chown_upload_mode=0755
```

18. iMG Deployment Models

There are three types of deployment models:

- Access Islands
- Multiple ISPs (Open Access)
- VLANs Providing More Than One Service

18.1 Access Islands

Since a large deployment of RGs can involve many business customers and residential subscribers, there is a network hierarchy model that, when used and labeled correctly, can help network administrators set up and track the high number (up to many thousand) of RGs. Refer to the following figure.

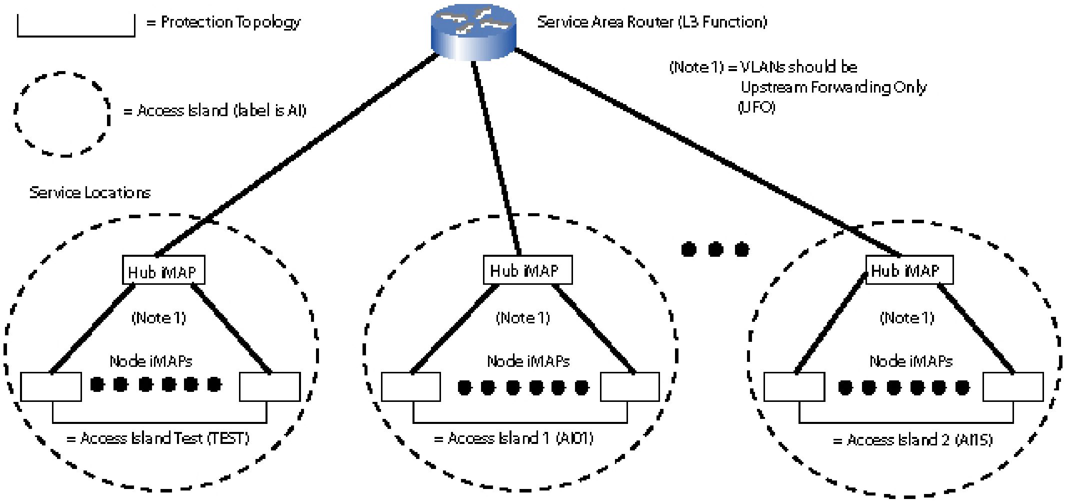


FIGURE 18-1 Network Hierarchy Model for Large Deployment of RGs - Access Islands

For each service provider's wiring center exchange, there can be a Provider Edge-Access Network (PE-AN), and these can be divided into Multi-service **Access Island** Networks. These Access Islands are basically one leaf of the larger network, and can be the initial configuration when a small number of RGs are initially deployed. With growth, a PE-AN could service, for example, 15,000 customers, which each island supporting 1000.

Note: So with this configuration, there can be up to 15 Access Island networks. This concept is used during provisioning.

Usually, one or two GbE or 10GbE Level-3 routers (PE-R) can be used to service the entire PE-AN; with this design the number of anticipated advanced subscriber services will determine the size and capabilities of the required provider edge router.

Note: Each Access Island uses a set of VLAN numbers unique to that Access Island; the next Access Island uses VLAN numbers that are usually the next number up. For example, Access Island one (AI01) could use a set of VLANs (201, 301, 401, 501, and 601) for DHCP discovery and the subscriber services. The next Access Island would use 202, 302, etc. The exception would be when the PE Router (L3) supports a Virtual Routing Function (VRF) and therefore sufficient multicast routing capabilities.

Then each Access Island could have the same VLAN configuration (mirror configuration). The one-hundred level VLANs (200, 300 etc.) could be for testing with the prefix TEST.

Note: When provisioning with Profiles for each Access Island, the only Profiles that are unique to each Access Island are the General Profiles, since the General Profile contains the VLAN and L3 static route information. The other Profiles (for service types) are usually the same for RGs in any Access Island since the service offered would have the same attributes.

18.2 Multiple ISPs (Open Access)

In networks where there are multiple service providers for various services, each VLAN may be used for a service type and ISP. The result is a set of VLANs for each service type, as shown in the following figure.

Refer to "Provisioning Guidelines for Models" on page 796 for details on the multiple ISP configuration.

Note: The default is the Access Island model.

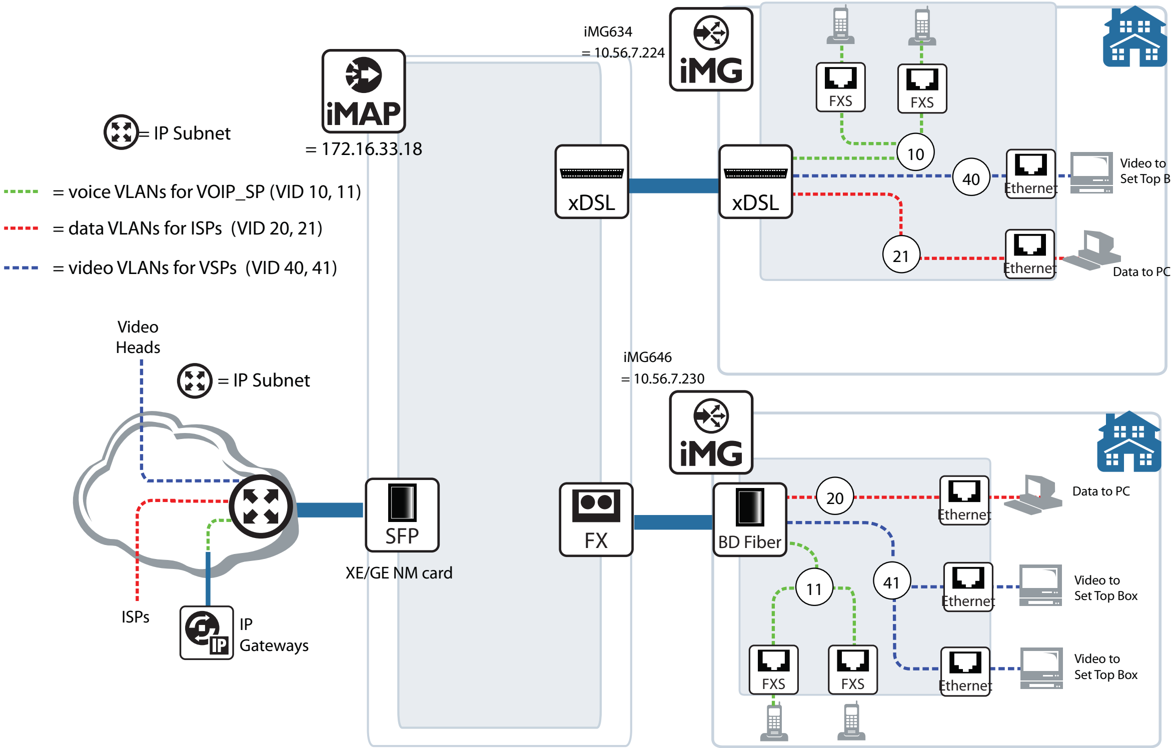


FIGURE 18-2 Multiple ISP Configuration

18.3 VLANs Providing More Than One Service

A VLAN can also be configured to support more than one service. The following figure shows an example of this.

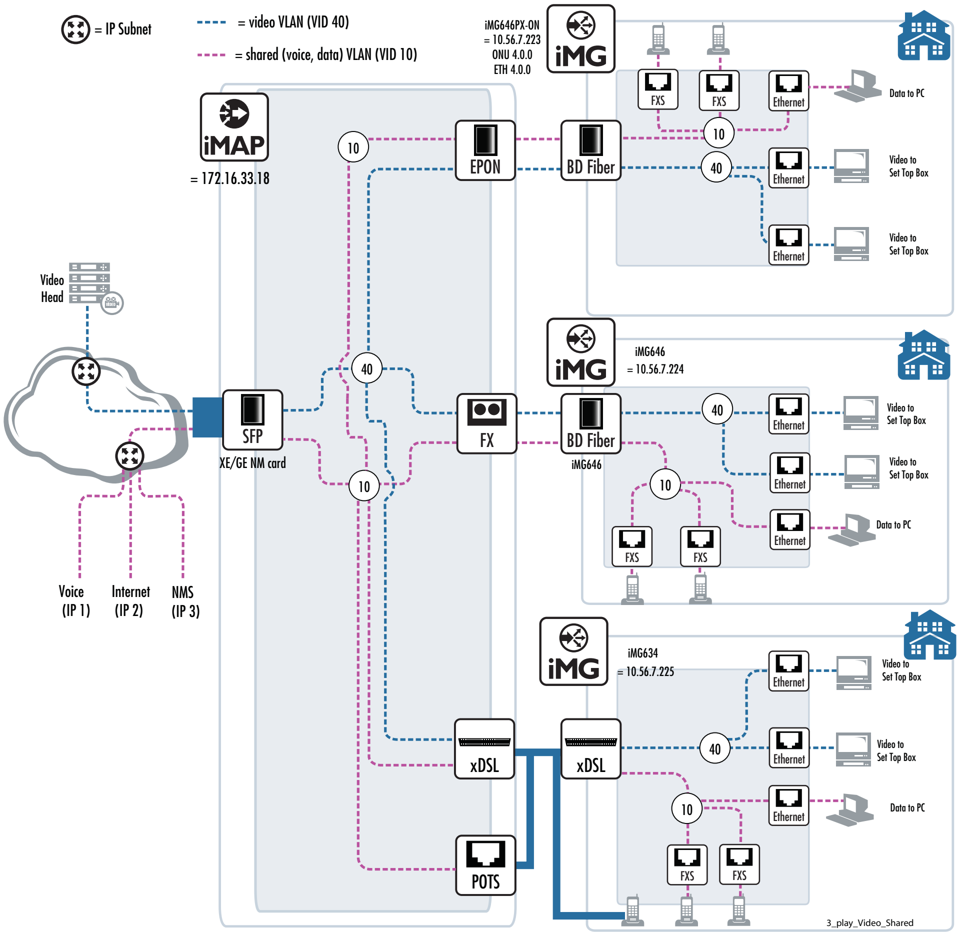


FIGURE 18-3 Multi-service VLAN

In Figure 18-3, one VLAN, 10, provides multiple services, data and voice. The services are separated by the provider (and the AlliedView NMS) using the IP address. The other VLAN, 40, provides video only and so all data packets in the VLAN can be sent to a video provider.

This type of configuration has variations, in which different types of services are on the one shared VLAN, and the service type on the single VLAN can vary. Datafilling this configuration is most easily done using the RG Profile Forms. Refer to "Configuring multi-service VLAN" on page 853.

19. iMG Profiles

The NMS allows you to create seven types of iMG service profiles. Each profile contains settings and attributes for a particular service. The seven profile types are:

- iMG General Profile
- iMG Internet Profile
- iMG Video Profile
- iMG Voice Profile
- iMG CES Profile
- iMG CES-DS1 Port Profile
- iMG CES-E1 Port Profile

Note: *The terms “RG” and “iMG” are used interchangeably in both the NMS client user interface and in this document. Unless explicitly stated, anything that applies to an iMG applies to an RG, and vice versa.*

19.1 Prerequisites

Before Profiles can be created, the administrator has already done the following:

- The DHCP servers and DNS servers have been set up
- Routing has been set up
- The G6 setup and if required with the IP address of BBI and AI's default router IP for voice subnet
- Knowledge of the “back office” management subnets
- Knowledge of the vpn “back office” management subnet

Note: *These “back office” subnets are separate subnets that ensure that it is possible to communicate with the RG. These require separate routes as well. Refer to "iMG General Profile" on page 702.*

- The service VLANs have been set up on the relevant iMAPs.
- Set of RG Profile names that will be used. For General RG Profiles the following shows the naming convention.

  For Access Island 1 (AI01)

- SPSI-AI00-P_1I_1V (Phone, 1 Internet, 1 video)
- SPSI-AI00-P_1I_2V (Phone, 1 Internet, 2 video)

  For Access Island 1:

- SPSI-AI00_1I_2V (1 Internet, 2 video)
- SPSI-AI00_1I_3V (1 Internet, 3 video
- etc....

Note: *Because rate limiting may be a factor the name may need to highlight this as well.*

Note: *“Packaged” marketing terms may also be appropriate names here, such as “DVLK-AI01-DSLPro+VVid”*

19.2 iMG General Profile

The general profile contains the high level attributes for the iMG to support a set of services (data, video, voice). The names you give to the profiles should match the service set that the profiles supports.

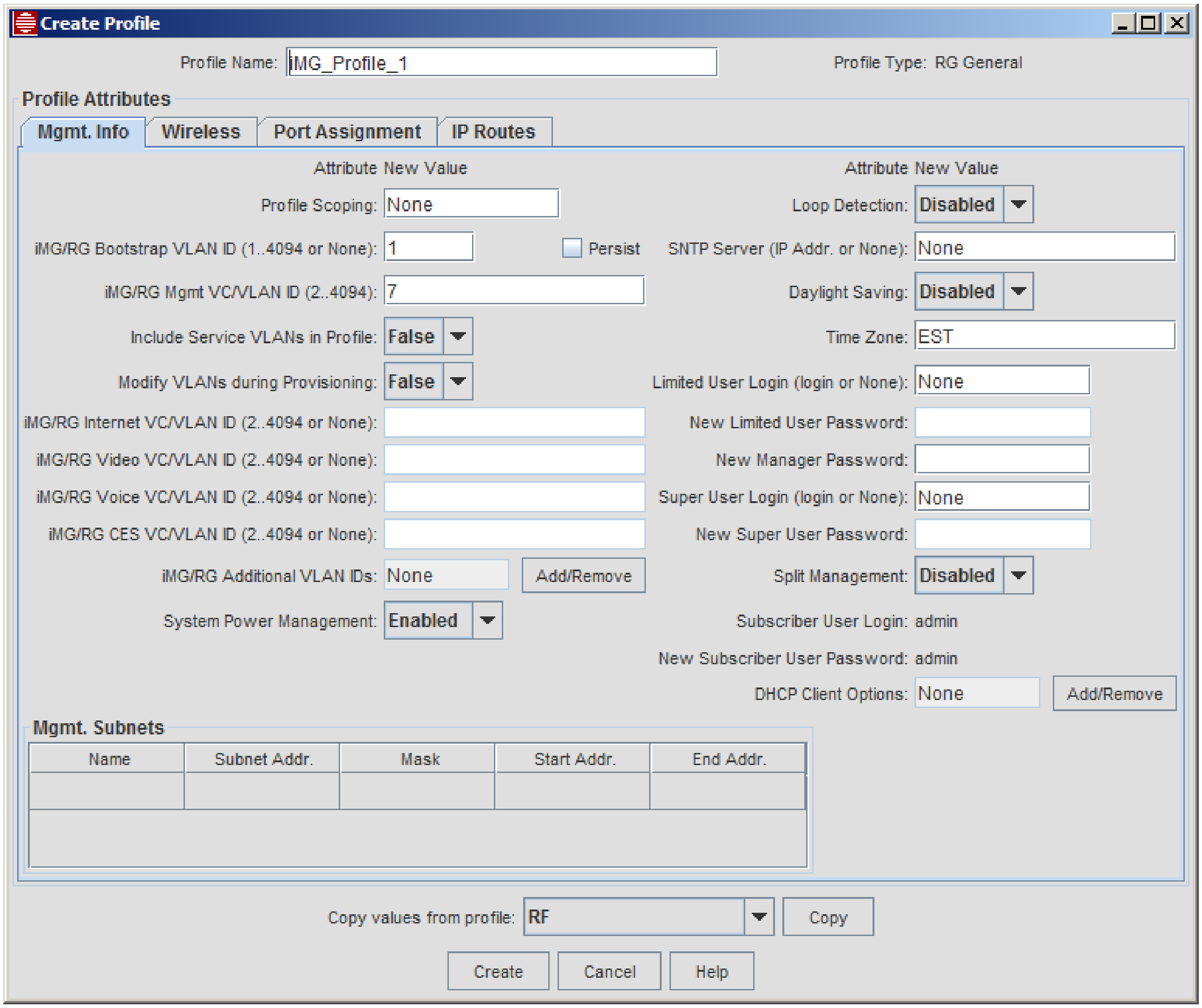
To create a general profile:

1. In the **Network Objects** panel, go to **Network Service Data** > **Profiles**.
2. From the menu, go to **Network Services** > **Profile** > **iMG/RG Service Profiles** > **Create iMG/RG General Profile**. The **Create Profile** box for the RG General profile appears.

The general profile contains four tabs:

- Mgmt. Info Tab
- Wireless Tab
- Port Assignment Tab
- IP Routes Tab

19.2.1 Mgmt. Info Tab



Create Profile

Profile Name: iMG_Profile_1

Profile Type: RG General

Profile Attributes

Attribute	New Value
Profile Scoping:	None
iMG/RG Bootstrap VLAN ID (1..4094 or None):	1 ☐ Persist
iMG/RG Mgmt VC/VLAN ID (2..4094):	7
Include Service VLANs in Profile:	False
Modify VLANs during Provisioning:	False
iMG/RG Internet VC/VLAN ID (2..4094 or None):	
iMG/RG Video VC/VLAN ID (2..4094 or None):	
iMG/RG Voice VC/VLAN ID (2..4094 or None):	
iMG/RG CES VC/VLAN ID (2..4094 or None):	
iMG/RG Additional VLAN IDs:	None
System Power Management:	Enabled

Attribute	New Value
Loop Detection:	Disabled
SNTP Server (IP Addr. or None):	None
Daylight Saving:	Disabled
Time Zone:	EST
Limited User Login (login or None):	None
New Limited User Password:	
New Manager Password:	
Super User Login (login or None):	None
New Super User Password:	
Split Management:	Disabled
Subscriber User Login:	admin
New Subscriber User Password:	admin
DHCP Client Options:	None

Mgmt. Subnets

Name	Subnet Addr.	Mask	Start Addr.	End Addr.

Copy values from profile: RF

FIGURE 19-1 RG General profile - Mgmt Info tab

TABLE 19-1 Create iMG General Profile - Mgmt InfoTab

Attribute	Value
Profile Name	A descriptive name that should match the service/function provided The prefix of profile name should start with a short but meaningful name that indicates the routing function and the Access Island and the service potential of the general profile, with the number of ports. Refer to Prerequisites. This is used for scoping. SPSI-AI01-1I_2V_3T (VoIP Telephone, 1 Internet, 2 Video, 3TLS) Profile names can only be up to 20 characters. To include all services, the administrator may need to delete an underscore. This is OK as long as the prefix works for scoping.
Profile Scoping	When used in conjunction with the Triple-Play form, controls the profiles available after selecting the device.port, or controls the device.port available after selecting the Profile.
iMG/RG Bootstrap VLAN Id	The default VLAN on the RG that is used when sending the original Discover Message. This is "out of the box" (factory configuration). This is used only through bootstrap.
Persist Checkbox	Used to retain the bootstrap VLAN at the end of triple play provisioning to aid in the replacement of faulty CPE. It can also put the bootstrap VLAN on the port when the profile (with Persist checked) is applied to the port from the View/Modify screen or deployed from the deploy profile tool.
iMG/RG Mgmt VLAN ID	The VLAN used for subsequent downloads once communication is established with the AlliedView NMS. It is derived from the im.conf file.
Include Service VLANs in Profile	Controls which network model is to be used. True - Access Island model is being used, and service VLAN fields are activated. False - Open Access model is being used, and service VLAN fields are de-activated.
Modify VLANs during Provisioning	Allows you to set customer-specific VLAN IDs. True - Enables fields on the Provision New Triple Play Customer box to enter customer-specific VLAN IDs. If services are assigned to ports and this setting is true, the VLAN ID fields on the Triple Play form are required for the assigned services. False - Customer-specific VLAN IDs are not required. If **Include Service VLANs in Profile** is set to True, the NMS uses the default VLAN ID values.
iMG/RG Internet VC/VLAN ID	The VLAN used for internet type service
iMG/RG Video VC/VLAN ID	The VLAN used for video type service
iMG/RG Voice VC/VLAN ID	The VLAN used for voice type service
iMG/RG CES VC/VLAN ID	The VLAN used for CES type service
iMG/RG Additional VLAN IDs	Shows VLAN IDs for custom VLANs. Use the Add/Remove button to open the Additional VLANs panel. Note that port service must be set to "None" to add an additional VLAN to the iMG. Refer to Provisioning Custom VLANs.
System Power Management	Enabled or disabled. Refer to System Power Management.

TABLE 19-1 Create iMG General Profile - Mgmt InfoTab (Continued)

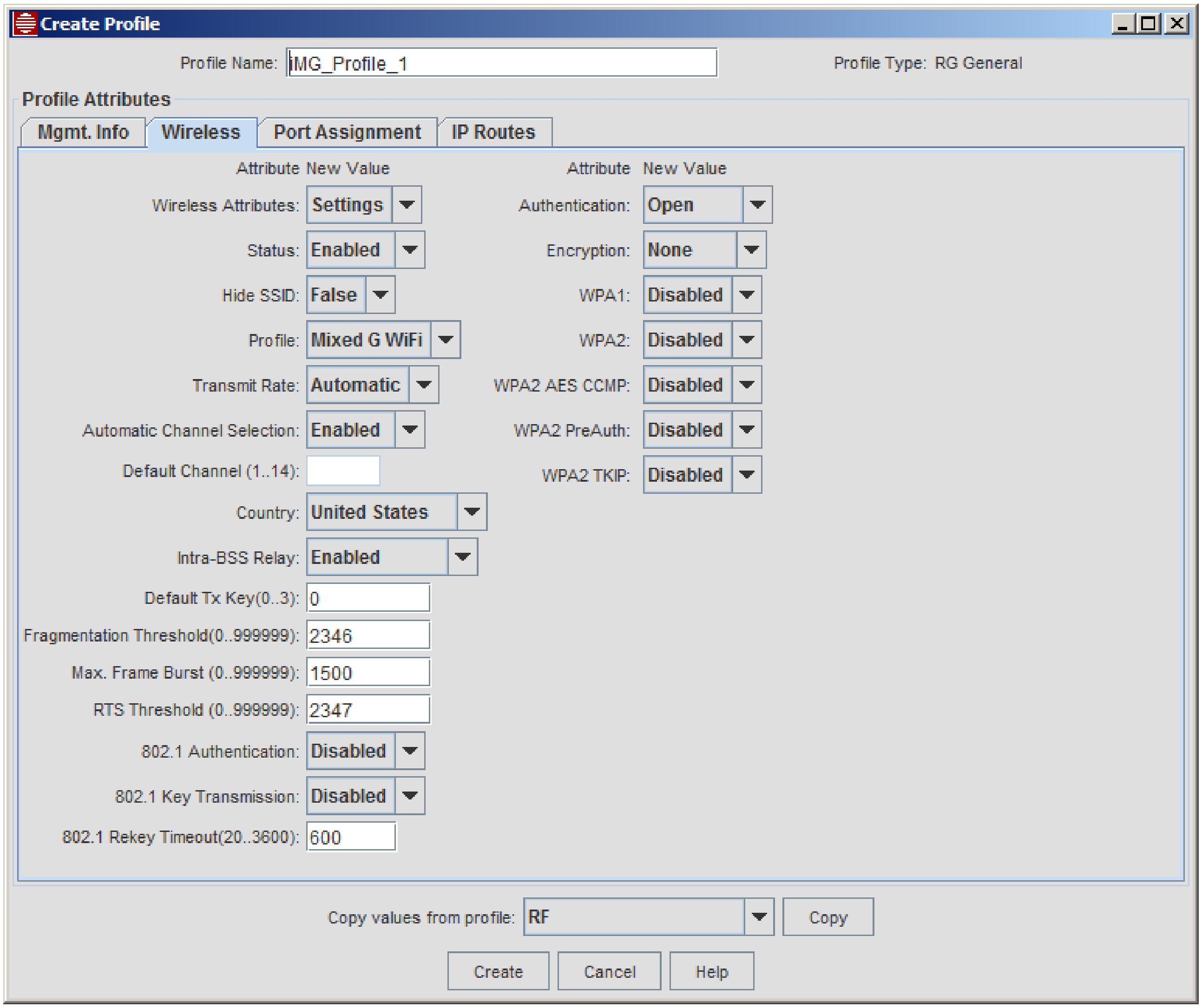
Attribute	Value
Loop Detection	Loop detection is intended to detect layer-2 loops in subscriber networks. When enabled, loop detection will disable the port where the symptom is detected before the loop does damage to the service provider's network. Loop detection is available on all switch interfaces on iMGs running software release 4.3 and above. On iMGs running software release 2.x or 3.x, loop detection is supported on 10M half-duplex links and is intended to support Ethernet links that have baluns connected.
SNTP Server	The IP address for the SNTP server, used to derive the correct time and time settings. (Default is None.)
Daylight Saving	Enables or Disables the Daylight Savings Feature for the iMG/RG. Note that this is only for devices on release 3-7 and up. This is also available on the Services Management Window.
Time Zone	Time Zone for the iMG, for example EST for Eastern Standard Time. For TR-069 CPEs, this is determined by the SNTP server setting, and so SNTP Server must be filled in first. If no SNTP server is provisioned, the iMGs default to “clock.fmt.he.net”.
Limited User Login	User ID of user with limited capabilities
New Limited User Password	Password for the Limited User
New Manager Password	Password for the user that the AlliedView NMS uses when it provisions the device. The userID is part of AlliedView NMS, has super user privileges, and cannot be changed.
Super User Login	The super user that can be created and changed by the administrator.
New Super User Password	The password for the Super User.
Split Management	A subscriber (rather than an NMS administrator) can configure wireless parameters on wireless iMG devices. Refer to Split Management for Wireless iMGs.
DHCP Client Options	DHCP client options for the service. Options 3 and 121 are supported. Option 3 is enabled by default in the iMG. Use Add/Remove to open the DHCP Client Options box. You can enable or disable each option listed.
Mgmt. Subnets	Controls what IP addresses are allowed to log into the iMG/RG using CLI or the iMG/RG’s web-based GUI. If no values are entered, any IP address can access the iMG/RG (using a login ID and password). Once at least one value is entered, the AlliedView NMS will add its own entry. Name - A name to identify the subnet. This cannot being with a digit. Subnet Address - An IP address. Used with the Mask Field to define a range. Mask - The mask used with the Subnet Address to define a range. Start Address - The first address in a range End Address - The last address in a range.
Copy values from profile	To create a new profile based on values from an existing profile, select an existing profile from the drop-down list. The fields will pre-populate with the values from the selected profile. Modify any fields as necessary for the new profile.
Create	Creates the profile.
Cancel	Closes the window without creating the profile. The values are not saved.

Note: *To configure the network as depicted in Figure 18-1, the RG General Profile should represent a specific Access Island (a group of iMAPs sharing a common set of VLANS and router[s]), so the Profile is defining Level-3 details and the VLAN values associated with it. Therefore if you had 4 access Island you would have 4 general profiles. This is assuming Virtual Routing is not in use.*

Note: *For the RG613, RG656, and the iMG646, only the manager password should be changed. (This is because a password can only be changed by switching to the user for that password. If the administrator changes the password for the Limited User (with the switching to the Limited User), the RG cannot switch back to Manager User. As a result, if the password for the Limited User is changed first, and then the Manager User password is changed within 5 minutes, there will be a time-out and the Manager User password will not be changed. (Waiting 5 minutes between these actions, or changing the Manager User first allows both changes to be made.)*

19.2.2 Wireless Tab

The Wireless tab in the iMG General profile configures wireless settings for iMGs running software release 3-x or earlier. Wireless settings for iMG 1000 and iMG 2000 series devices are configured in the iMG Internet profile. To configure wireless settings for iMG 1000 and iMG 2000 series devices, see "Wireless Tab" on page 726.



Profile Name: iMG_Profile_1

Profile Type: RG General

Attribute	New Value	Attribute	New Value
Wireless Attributes:	Settings	Authentication:	Open
Status:	Enabled	Encryption:	None
Hide SSID:	False	WPA1:	Disabled
Profile:	Mixed G WiFi	WPA2:	Disabled
Transmit Rate:	Automatic	WPA2 AES CCMP:	Disabled
Automatic Channel Selection:	Enabled	WPA2 PreAuth:	Disabled
Default Channel (1..14):		WPA2 TKIP:	Disabled
Country:	United States		
Intra-BSS Relay:	Enabled		
Default Tx Key(0..3):	0		
Fragmentation Threshold(0..999999):	2346		
Max. Frame Burst (0..999999):	1500		
RTS Threshold (0..999999):	2347		
802.1 Authentication:	Disabled		
802.1 Key Transmission:	Disabled		
802.1 Rekey Timeout(20..3600):	600		

Copy values from profile: RF

FIGURE 19-2 iMG General Profile - Wireless Tab

TABLE 19-2 Create iMG General Profile - Wireless Tab

Attribute	Value	Default
Wireless Attributes	The selection made here controls which fields appear on the Provision New Triple Play Customer form. Settings - Wireless attributes are not displayed when provisioning a new customer. The values set in the profile are used. Defaults - Wireless attributes from the profile are displayed on the provisioning screen for review and can be modified when provisioning a new customer. After the customer is provisioned, you can view and modify wireless attributes from the Wireless view/modify screen.	Settings
Status	Enable or disable the wireless interface on the device. When the wireless network is disabled, the wireless network can be seen but connections are not allowed.	Enabled
Hide SSID	Hide the SSID. False - The SSID is broadcast. True - The SSID is hidden.	False
Profile	Specifies the wireless profile for the device. Mixed G WiFi - 2.4 GHz 802.11g/b Dynamic Non-ERP B Only - 2.4 GHz 802.11b G Only - 2.4 GHz 802.11g without Non-ERP	Mixed G WiFI
Transmit Rate	Specifies the transmit rate. Automatic - The driver determines the optimal transmit rate. X Mbps - The specific transmit rate. Options are 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 or 54.	Automatic
Automatic Channel Selection	Automatically select the best channel when the device starts up. False - Disable automatic channel selection. True - Enable automatic channel selection.	Enabled
Default Channel	The default channel to use. The default value should be the minimum allowed for the band.	
Country	The 802.11d country string for the wireless card.	United States
Intra-BSS Relay	Specifies whether or not to use intra-bss relay. Enabled - Use intra-bss relay. Disabled - Do not use intra-bss relay. Client Isolation - Enable wireless L2 Client Isolation (intra-bss drop).	Enabled
Default Tx Key	Specifies which encryption key to use by default.	0
Fragmentation Threshold	Specifies the threshold over which frames are fragmented.	2346
Max. Frame Burst	Specifies the threshold for Nitro frame bursting into the iMG.	1500
RTS Threshold	Specifies the threshold over which frames use the RTS/CTS mechanism.	2347

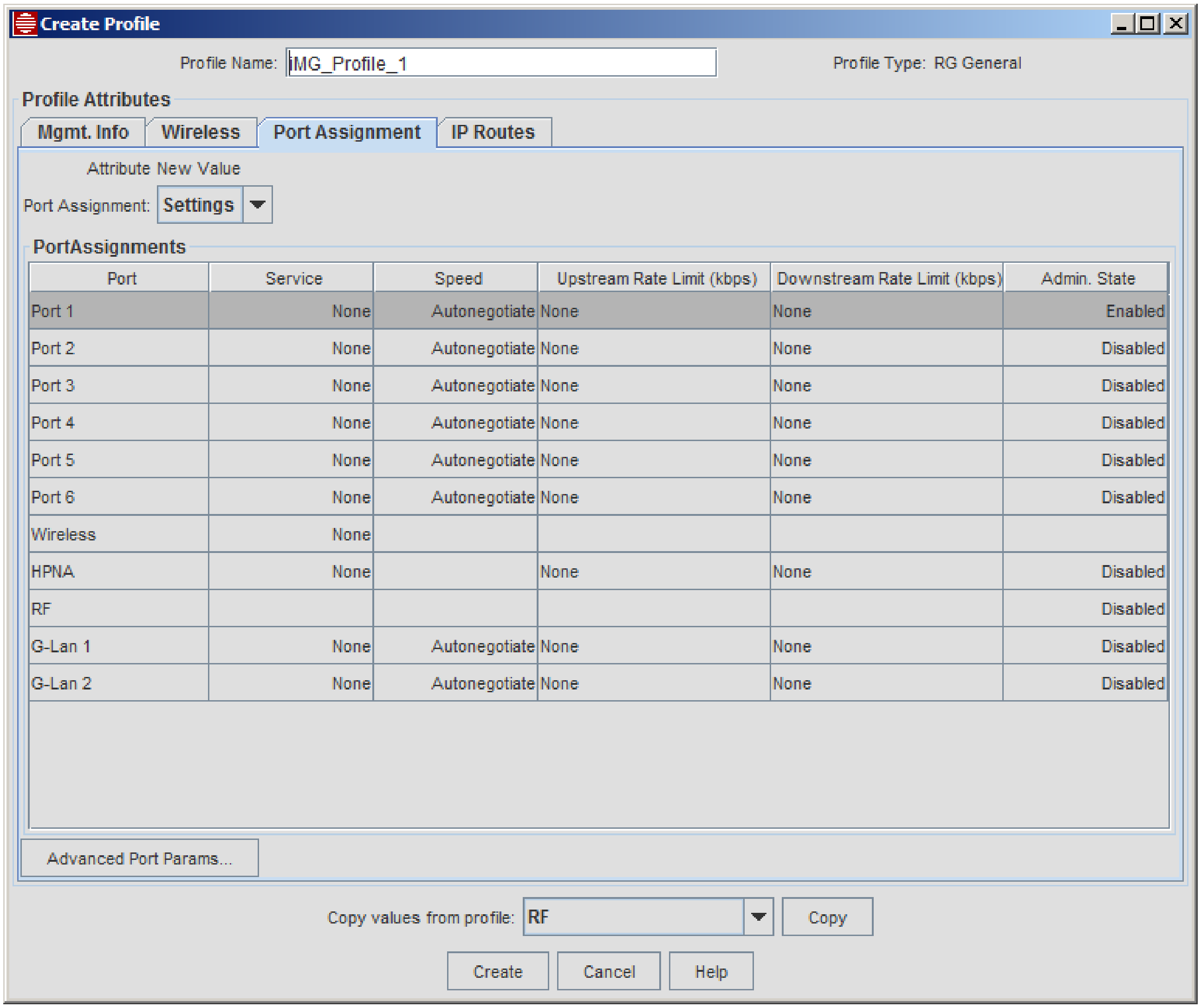
TABLE 19-2 Create iMG General Profile - Wireless Tab (Continued)

Attribute	Value	Default
802.1 Authentication	Specifies whether to use 802.1 authentication in the wireless network. Disabled - Do not use 802.1 authentication on the iMG. Enabled - Set the iMG as authenticator in a WPA/WPA2 system wireless network.	Disabled
802.1 Key Transmission	Specifies whether or not to use key transmission according to 802.11 specifications. Enabled - Use key transmission. Disabled - Do not use key transmission.	Disabled
802.1 Rekey Timeout	Specifies the WEP rekey timeout to initiate a new WEP key for the session. The timeout should be set to rotate the keys fast enough to prevent an attacker from sniffing enough packets to discover the WEP key.	600
Authentication	Specifies the authentication framework for the network. Open - Use an open access authentication framework. Credentialed authentication is not required. Shared - Use a shared key authentication framework. WPA-PSK - Use a WPA/WPA2 authentication framework.	Open
Encryption	Specifies the encryption method. None - No encryption is used. WEP-64 - Use WEP 64-bit encryption. WEP-128 - Use WEP 128-bit encryption.	None
WPA1	Specifies whether to use WPA1 security protocols. Enabled - Use WPA1 security. Disabled - Do not use WPA1 security.	Disabled
WPA2	Specifies whether to use WPA2 security protocols. Enabled - Use WPA2 security. Disabled - Do not use WPA2 security.	Disabled
WPA2 AES CCMP	Specifies whether to use WPA2 AES CCMP security protocols. Enabled - Use WPA2 AES CCMP security. Disabled - Do not use WPA2 AES CCMP security.	Disabled
WPA2 PreAuth	Specifies whether to use WPA2 PreAuth security protocols. Enabled - Use WPA2 PreAuth security. Disabled - Do not use WPA2 PreAuth security.	Disabled
WPA2 TKIP	Specifies whether to use WPA2 TKIP security protocols. Enabled - Use WPA2 TKIP security. Disabled - Do not use WPA2 TKIP security.	Disabled
Copy values from profile	To create a new profile based on values from an existing profile, select an existing profile from the drop-down list. The fields will pre-populate with the values from the selected profile. Modify any fields as necessary for the new profile.	

TABLE 19-2 Create iMG General Profile - Wireless Tab (Continued)

Attribute	Value	Default
Create	Creates the profile.	
Cancel	Closes the window without creating the profile. The values are not saved.	

19.2.3 Port Assignment Tab



Profile Name: iMG_Profile_1

Profile Type: RG General

Attribute New Value

Port Assignment: Settings

PortAssignments

Port	Service	Speed	Upstream Rate Limit (kbps)	Downstream Rate Limit (kbps)	Admin. State
Port 1	None	Autonegotiate	None	None	Enabled
Port 2	None	Autonegotiate	None	None	Disabled
Port 3	None	Autonegotiate	None	None	Disabled
Port 4	None	Autonegotiate	None	None	Disabled
Port 5	None	Autonegotiate	None	None	Disabled
Port 6	None	Autonegotiate	None	None	Disabled
Wireless	None				
HPNA	None		None	None	Disabled
RF					Disabled
G-Lan 1	None	Autonegotiate	None	None	Disabled
G-Lan 2	None	Autonegotiate	None	None	Disabled

Copy values from profile: RF

FIGURE 19-3 RG General Profile - Port Assignment Tab

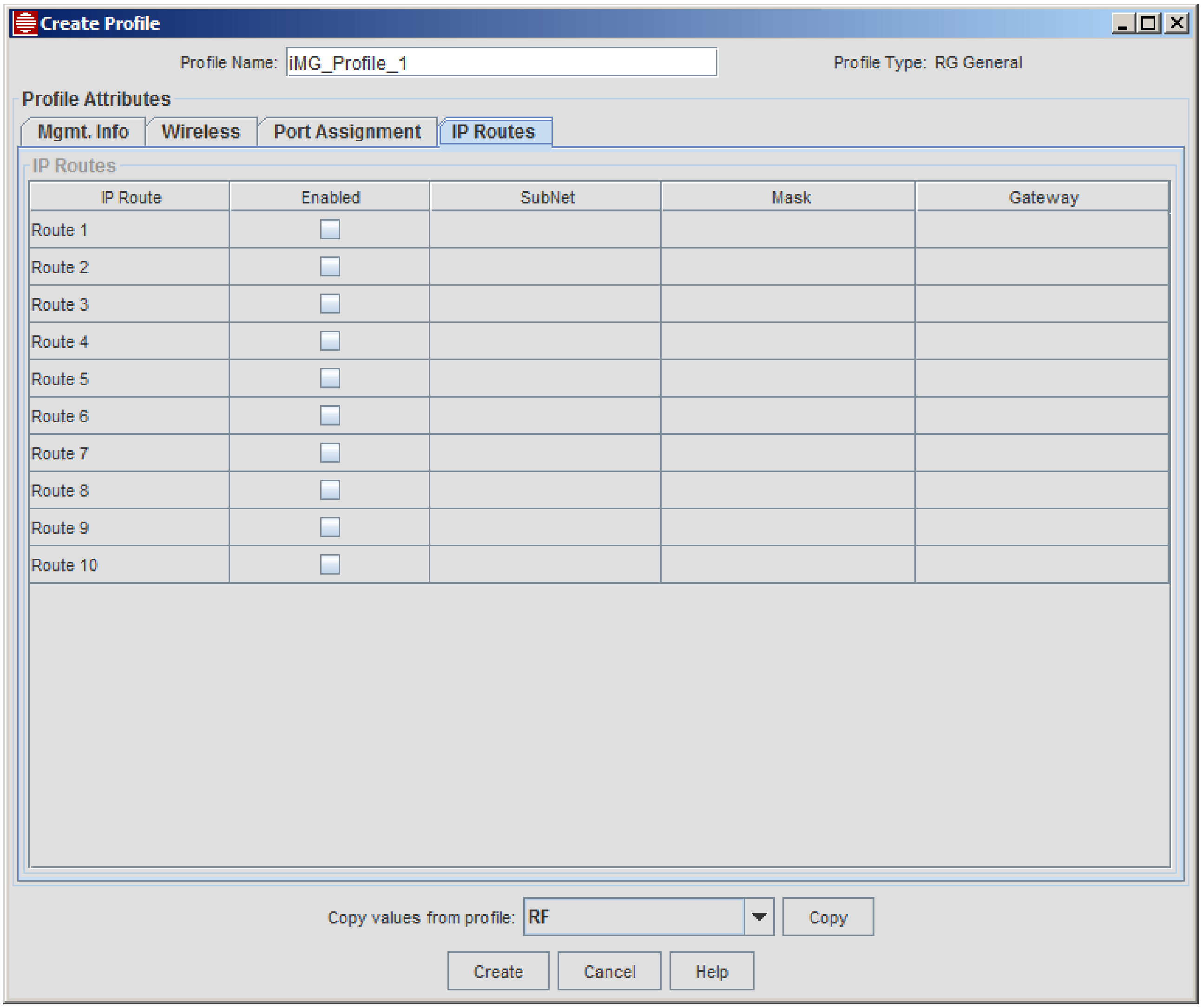
TABLE 19-3 Create iMG General Profile - Port Assignment Tab

Attribute	Value
Port Assignment	The selection made here controls which fields appear on the Provision New Triple Play Customer form. Settings - Port assignments will not be displayed when provisioning a new customer. The values as set in the profile will be used. Defaults - Port assignments from the profile will be displayed on the provisioning screen for review and can be modified when provisioning a new customer. After the customer is provisioned, you can view and modify port assignments from the Port Management view/modify screen.
Port	The ports associated with the device. Ports 1-6 - The LAN ports on the device. Wireless - This port is available on wireless devices only. HPNA - This port is available on the iMG6x6MOD. Refer to Configuration 7 - iMG7x6MOD with HPNA. RF - G-Lan 1-2 - These ports are available with the 1 Gigabit WAN with RJ-45 LAN card to provision services on the G-Lan ports.
Service	The type of service to configure on the port during provisioning. None - No service will be configured on the port. Internet - A data service (type not determined here) will be configured on the port. TLS - Transparent LAN Service will be configured on the port. Video - A video service (type not determined here) will be configured on the port. Voice - A VoIP phone is connected to the LAN port (configured on Voice VLAN) This service is not available on the HPNA port. Internet/Video - For Media Room. In this configuration, a new service is configured for a LAN port called "'Internet/Video" to indicate that the port can be used for video or data traffic. Management -
Speed	The following speed settings are available: • Autonegotiate - The line will chose the maximum speed and direction it can support. • Coax - Used for P2P RG59 + RG6 coax (10 Meg Full Duplex) in a star/hubspoke top with software loop detection. • 1G Full • 1G Half • 100M Full • 100M Half • 10M Full • 10M Half
Upstream Rate Limit (kbps)	Speed in kbps for the maximum upstream rate.
Downstream Rate Limit (kbps)	Speed in kbps for the maximum downstream rate.

TABLE 19-3 Create iMG General Profile - Port Assignment Tab (Continued)

Attribute	Value
Admin. State	These are set in the General Profile. As with other parameters in the profile, if the admin state in the profile differs from that on the iMG, then a profile out of sync alarm is generated on re-discovery. For profiles that existed before this enhancement, the admin state for ports that have a service is set to enabled, and for those ports without a service, the admin state is set to disabled.
Advanced Port params	Brings up specific features: - Disable on Power Failure feature for the port. Refer to "LAN Ports Power Management" on page 899. - Flow Control - Refer to "Flow Control" on page 902 - DSCP Status - Enables the support of DSCP IP field on the incoming frames. Refer to the *Allied Telesis Gateway Product Family Software Reference*, command SWITCH SET SUPPORT DSCP. - Protect - Refer to "Protected Ports" on page 905. - Additional Untagged VLAN IDs - Refer to "Provisioning Custom VLANs" on page 818. - Additional Tagged VLAN IDs - Refer to "Provisioning Custom VLANs" on page 818.
Copy values from profile	To create a new profile based on values from an existing profile, select an existing profile from the drop-down list. The fields will pre-populate with the values from the selected profile. Modify any fields as necessary for the new profile.
Create	Creates the profile.
Cancel	Closes the window without creating the profile. The values are not saved.

19.2.4 IP Routes Tab



Profile Name: iMG_Profile_1

Profile Type: RG General

IP Route	Enabled	SubNet	Mask	Gateway
Route 1	□			
Route 2	□			
Route 3	□			
Route 4	□			
Route 5	□			
Route 6	□			
Route 7	□			
Route 8	□			
Route 9	□			
Route 10	□			

Copy values from profile: RF

FIGURE 19-4 RG General Profile - IP Routes Tab

TABLE 19-4 Create iMG General Profile - IP Routes Tab

Attribute	Value
IP Route	IP Routes that are available for the RG The user should always create a route to the “back office” management subnets. (The AlliedView has one as well that is unavailable to the user.)
Enabled	Activates the other IP Route Fields
Subnet	Subnet address
Mask	Mask over the subnet address, usually 255.255.255.0
Gateway	IP address for the Gateway server
Copy values from profile	To create a new profile based on values from an existing profile, select an existing profile from the drop-down list. The fields will pre-populate with the values from the selected profile. Modify any fields as necessary for the new profile.

TABLE 19-4 Create iMG General Profile - IP Routes Tab

Attribute	Value
Create	Creates the profile.
Cancel	Closes the window without creating the profile. The values are not saved.

Note: *The administrator should also add route(s) that include the entire scope of management subnets that will require "direct" access to RGs. (The AlliedView NMS will always have direct access but TAC/NOC Staff with their PCs/workstations may not unless specifically included in a route.*

Note: *For Media Room, the routes table in General profile allows up to 10 different routes in the iMG because media room devices connected to the iMG may request services configured in separate subnets on the upstream network.*

19.3 iMG Internet Profile

The Internet profile allows you to set up security for Internet traffic. The security system provides a single point of control for all traffic entering and leaving the private network.

To create an Internet profile:

1. In the **Network Objects** panel, go to **Network Service Data** > **Profiles**.
2. From the menu, go to **Network Services** > **Profile** > **iMG/RG Service Profiles** > **Create iMG/RG Internet Profile**. The **Create Profile** box for the RG Internet profile appears.

The iMG Internet profile contains the following tabs:

- General Internet Info Tab
- Security Tab
- Firewall Tab
- NAT Tab
- Wireless Tab

You must configure settings in all tabs to create a comprehensive security profile. The Wireless tab only pertains to iMGs with wireless capablities.

The security system has the following main parts:

- Enable and disable all areas of the security system (NAT and Firewall tabs).
- Add IP interfaces to the Security tab that are used to configure the NAT and Firewall tabs.
- **Triggers** - Triggers are user to inform the security mechanism to expect secondary sessions and handle the situation dynamically, allowing the secondary sessions for data flow for the duration of the session. The user configures the iMG/RG with a range of primary port number(s).The Primary port number refers to the TCP/UDP port number to which the primary (starting) session of the application is established. During session set up, if there is a local host that was expecting the incoming session, then the session is established. If a local host is not found, then the packet is discarded. This mechanism enables the iMG/RG to allow in only those incoming secondary sessions that should be allowed in, and can reject malicious attempts to establish incoming sessions.
- **Timeout** - When a session using a secondary port is being closed, an exchange of FIN, FIN/ACK packets stops passing packets for that session. For cases where this does not occur (UDP, or one end is simply turned off), the user can configure a period of inactivity before the session is closed and the iMG/RG will no longer forward packets for the session.
- **Session Chaining** - Some applications spawn their own secondary sessions. This process is known as session chaining. When secondary sessions are successfully established, the source/destination addresses of the session will also be added to the table of currently open primary sessions.

- **Firewall** - The Firewall feature ensures that only traffic that has been already defined is allowed to access the internal network. This is done by provisioning the following:
- **Port Filters** - These are port attributes that define:

  - What protocol type is allowed (specified using the protocol number or the protocol name)

  - The range of source and destination port numbers allowed

  - The direction that packets are allowed to travel in (inbound, outbound, neither, or both)

- **Validators** - How the Firewall handles packets based on the source/destination IP address.
- **Intrusion Detection System (IDS)** - This protects the system from the following kinds of attacks:
  - **DOS (Denial of Service) attacks** - a DOS attack is an attempt by an attacker to prevent legitimate hosts from accessing a service.
  - **Port Scanning** - an attacker scans a system in an attempt to identify any open ports.
  - **Web Spoofing** - an attacker creates a 'shadow' of the World Wide Web on their own machine, however legitimate host sees this as the 'real' WWW. The attacker uses the shadow WWW to monitor the host's activities and send false data to and from the host's machine.

  There are parameters that are filled out to configure each type.

- **Network Address Translation (NAT)** - The basic NAT feature is that the devices in the internal network have their own IP addresses and yet access the external network using a separate internet address, and this is the only address devices on the external network see. Doing this provides both a conservation of public IP addresses and security. Security is provided by keeping an internal table of the source IP address and source port as well as a substitute source port number. Packets coming from the external network must include the substitute port number or the packet is dropped.

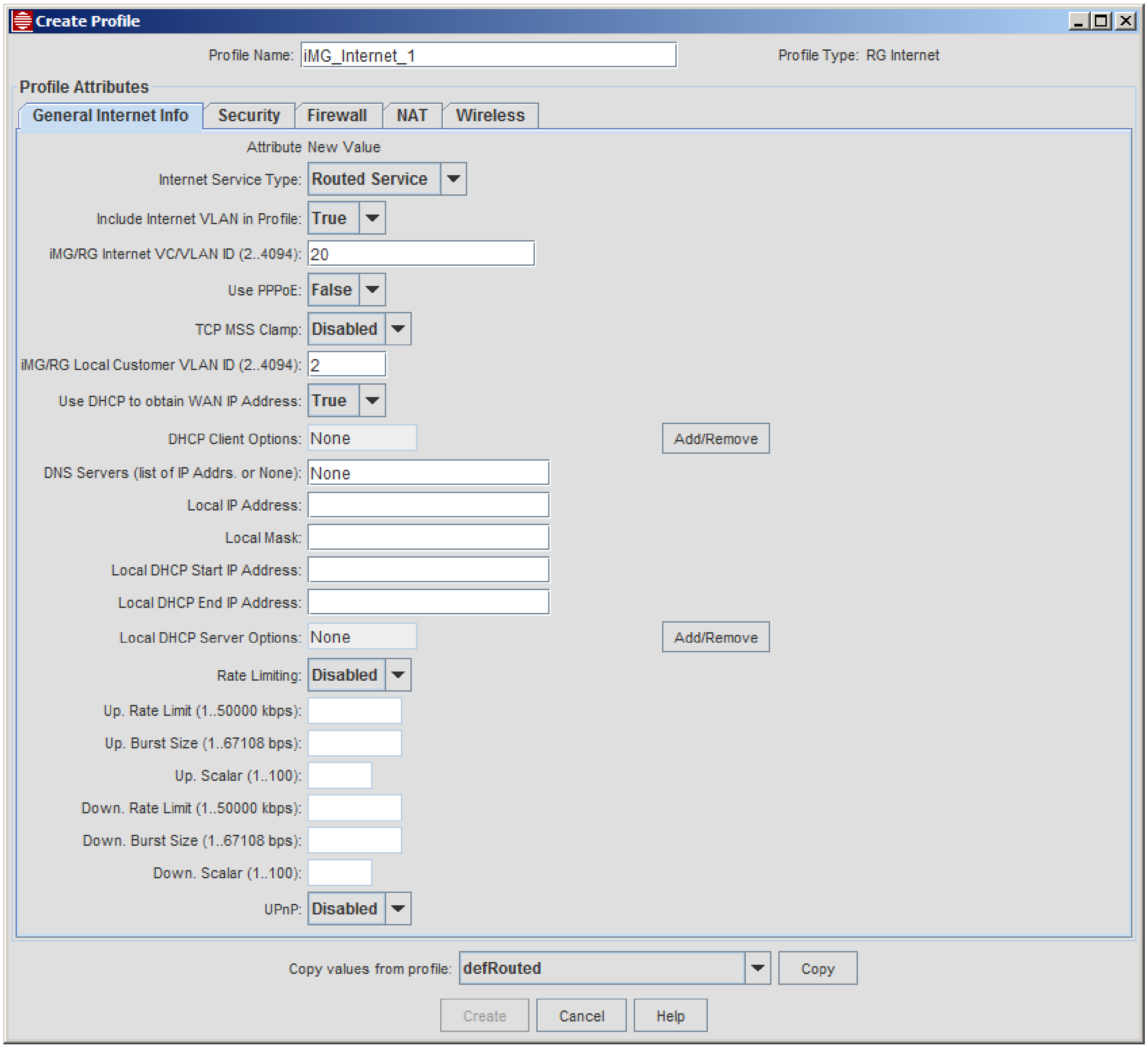
  In some cases, you need to set up static IP addresses/port mappings. This is done using Global Pools and Reserved Mappings.

- A **Global Pool** is a range of external IP addresses that are available, rather than one. The reason global pools are used is so that you can map an outside address to a specific internal interface. This is called reserve mapping.
- **Reserved Mapping** is used for mapping an IP address from the Global Pool to an individual address of a device in the internal network. When NAT receives a message, it uses its internal interface to forward the packet to the same port number on a selected internal computer, as well as any responses from the internal computer that are forwarded to the requesting external computer. Reserved mappings can also be used so that different internal hosts can share the same global address by mapping different ports to different hosts. For example, Host A is an FTP server and Host B is a Web server, and by mapping the FTP port to host A and an http port on Host B, both hosts can use the same external address.
- **Internet Key Exchange (IKE)** - To support NAT IPSec traversal, you specify how Internet Key Exchange (IKE) packets are translated. IKE establishes a shared security policy and authenticates keys for services that require keys, such as IPSec. Before any IPSec traffic can be passed, each router/firewall/host must verify the identity of its peer. The user specifies whether the source port will be translated for IKE packets, or IKE cookies are used to identify IKE sessions.
- **PPPoE** - You must enable PPPoE on an iMG 1000 or iMG 2000 series device from the Internet profile. Once an iMG 1000 or iMG 2000 series device is provisioned to use PPPoE, you can modify the PPPoE username and password, but you cannot disable PPPoE without deploying a new Internet profile or deprovisioning and reprovisioning the iMG.

Note: *You cannot use the Deploy Profile menu command to apply an Internet profile with PPPoE enabled to iMGs. You must apply these profiles from the iMG View/Modify screen, or when you initially provision an iMG with a new triple play customer.*

19.3.1 General Internet Info Tab

On the General Internet Info tab you specify a bridged or routed service.



Profile Name: iMG_Internet_1

Profile Type: RG Internet

Profile Attributes

Attribute	New Value
Internet Service Type:	Routed Service
Include Internet VLAN in Profile:	True
iMG/RG Internet VC/VLAN ID (2..4094):	20
Use PPPoE:	False
TCP MSS Clamp:	Disabled
iMG/RG Local Customer VLAN ID (2..4094):	2
Use DHCP to obtain WAN IP Address:	True
DHCP Client Options:	None
DNS Servers (list of IP Addrs. or None):	None
Local IP Address:	
Local Mask:	
Local DHCP Start IP Address:	
Local DHCP End IP Address:	
Local DHCP Server Options:	None
Rate Limiting:	Disabled
Up. Rate Limit (1..50000 kbps):	
Up. Burst Size (1..67108 bps):	
Up. Scalar (1..100):	
Down. Rate Limit (1..50000 kbps):	
Down. Burst Size (1..67108 bps):	
Down. Scalar (1..100):	
UPnP:	Disabled

Copy values from profile: defRouted

FIGURE 19-5 iMG Internet Profile - General Internet Info tab

TABLE 19-5 Create iMG Internet Profile General Internet Info Tab

Attribute	Value
Profile Name	A descriptive name that should match the service provided. Profiles that use the Access Island (AI) concept have the 'Include Internet VLAN in Profile' set to False. For the Open Access (OA) model, the field is set to True and a VLAN number can be entered in the 'iMG/RG Internet VLAN ID' field (2..4094). Example Names: • BasicHomeInetAI (Security, and therefore Firewall and NAT disabled) • BasicHomeInetOA (same as above but includes internet VLAN ID) • BusinessInetAI (Security and Firewall are Enabled but any attributes datafilled are not included as part of the Profile) • BusinessInetOA (same as above but includes internet VLAN ID) • BusinessStatic (Routed Service) • HomeNetworkingAI (Security, Firewall, and NAT are Enabled and any attributes datafilled are included as part of the Profile) • HomeNetworkingOA (same as above but includes internet VLAN ID) • Bridged Int Srv (Bridged Service)
Internet Service Type	Bridged Service Routed Service
Include Internet VLAN in Profile	The value entered here depends on the network model: False - The Access Island model is used, and the Internet VLAN Id field is blank. True - The Open Access model is used, and the Internet VLAN Id field is activated.
iMG/RG Internet VLAN ID (2..4094)	The VLAN that supports internet service. If the 'Include Internet VLAN in Profile' is set to True, this field is activated.
Use PPPoE	Determines whether the iMG will use PPPoE to connect to the ISP. False - The PPPoE protocol will not be used to establish the connection between the iMG and the ISP. True - The PPPoE protocol will be used to establish the connection between the iMG and the ISP. To activate the PPPoE field, the **Internet Service Type** must be set to **Routed Service**. When **Use PPPoE** is set to **True**, the **Use DHCP to obtain WAN IP Address** field is deactivated.
TCP MSS Clamp	When using the PPPoE client on the iMG, either the iMG or the PPPoE concentrator/RAS should be configured to clamp the maximum TCP MSS value. For PPPoE the maximum mss is 1452. Without this clamp, connectivity issues could occur, and access to some websites could fail. Refer to the *Allied Telesis Gateway Product Family Software Reference*.
Internet MTU	This does not appear on the Profile, but does show up on the Service Management form. The MTU is the Maximum Transmission Unit - the maximum packet size (in bytes) an interface can handle. The MTU should be set to a value appropriate for the transport attached to the interface (typically from 576 to 1500 bytes). Refer to the *Allied Telesis Gateway Product Family Software Reference* for more information.
iMG/RG Local Customer VLAN ID (2..4094)	VLAN that is local to the iMG only.
Use DHCP to Obtain WAN IP Address	If True, use DHCP Discovery to obtain the network-side IP address for the RG. If False, static IP provisioning and IP/masks must be manually entered.

TABLE 19-5 Create iMG Internet Profile General Internet Info Tab (Continued)

Attribute	Value
DHCP Client Options	DHCP client options for the service. Options 3 and 121 are supported. Option 3 is enabled by default in the iMG. Use Add/Remove to open the DHCP Client Options box. You can enable or disable each option listed.
DNS Servers (list of IP Addrs. or None)	DNS servers associated with the DHCP discovery
Local IP Address	The IP address of the iMG/RG for the LAN that it services. This and the remaining fields are activated only when NAT is enabled on the NAT tab.
Local Mask	The masking for the local IP addresses. Usually this is 255.255.255.0 so that the local addresses can range from 1 to 255.
Local DHCP Start IP Address	The first address in the range for a local device in the local network. This possible range must be derived from the local IP address and the local mask.
Local DHCP End IP Address	The last address in the range for a local device in the local network.
Local DHCP Server Options	DHCP server options for the service. Options 66 and 67 are supported. Both options are disabled by default in the iMG. Use Add/Remove to open the DHCP Server Options box. You can enable or disable and set a value for each option listed.
Rate Limiting	Enable or disable rate limiting. When enabled, the upstream and downstream attributes (Rate Limit, Burst Size and Scalar) are editable. The downstream rate limiting applies to Internet VLAN traffic and is used for wireless traffic because the downstream rates are applied on WAN port when the traffic enters the iMG. Upstream rate limiting applies to Local VLAN traffic which applies to LAN ports but not wireless because classifiers are applied on the transport and the wireless transport is not the same as LAN transport. Scalar represents the weight of each byte of data coming over the channel. The higher the scaler value the lower the worth each byte of data is counted for rate limiting purposes. This allows a more precise reflection of actual network traffic. For certain wireless IMG devices running software release 3.8 or higher, you can configure the upstream rate limits. Note that the NMS will use the same rate limit values that are currently set for wired ports on wireless. The devices that support this are: • iMG616-W • iMG634-A-W-R2 • iMG634-B-W-R2 These fields can also be changed on the Service Management form for these wireless devices.
Up. Rate Limit (1..50000 kbps)	The upstream rate limit.
Up. Burst Size (1..67108 bps)	The upstream burst size.
Up. Scalar (1..100)	The upstream scalar weight.
Down. Rate Limit (1..50000 kbps)	The downstream rate limit.
Down. Burst Size (1..67108)	The downstream burst size.

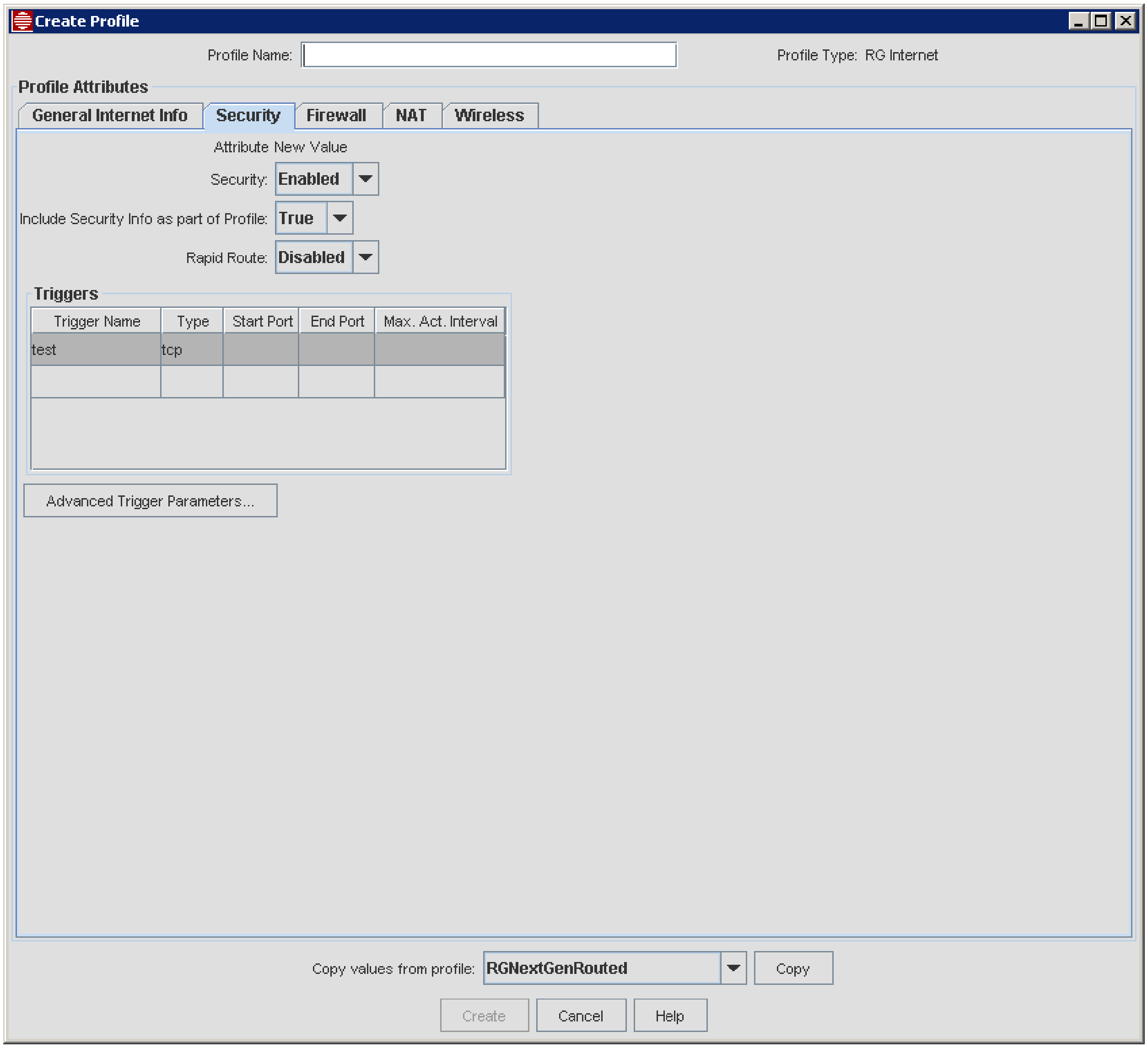
TABLE 19-5 Create iMG Internet Profile General Internet Info Tab (Continued)

Attribute	Value
Down. Scaler (1..100)	The downstream scalar weight.
UPnP	Enable or disable UPnP on the iMG. You can enable UPnP for either Internet or video service, but not both simultaneously. If UPnP is enabled on the Internet service it must be disabled on the video service, and vice versa.
Copy values from profile	To create a new profile based on values from an existing profile, select an existing profile from the drop-down list. The fields will pre-populate with the values from the selected profile. Modify any fields as necessary for the new profile.
Create	Creates the profile.
Cancel	Closes the window without creating the profile. The values are not saved.

19.3.2 Security Tab

The Security tab controls whether the security system and its subsystems are enabled, and if so, the attributes for these subsystems. If security is disabled, the following fields in the profile are also disabled:

- Firewall tab - Firewall field
- NAT tab - NAT field



Profile Name:

Profile Type: RG Internet

Profile Attributes

Attribute New Value

Security: Enabled

Include Security Info as part of Profile: True

Rapid Route: Disabled

Triggers

Trigger Name	Type	Start Port	End Port	Max. Act. Interval
test	tcp			

Copy values from profile: RGNextGenRouted

FIGURE 19-6 iMG Internet Profile - Security tab

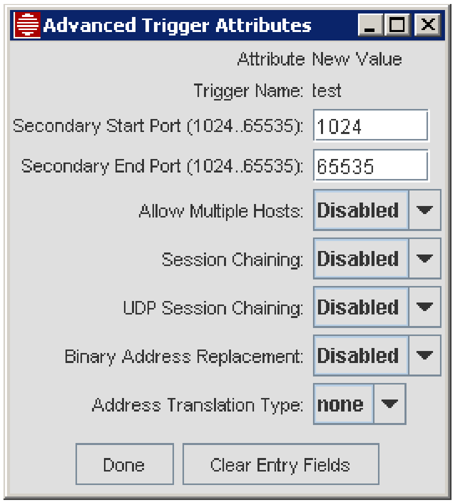
TABLE 19-6 Create iMG Internet Profile Security Tab

Attribute	Value
Security	Whether the feature is Enabled or Disabled. This option is activated only for Routed Service. Moreover, it controls whether the Enable/Disable fields for Firewall and NAT are activated. *Note: Security does not have to be enabled to enter Triggers and Mgmt. Stations, although this would not usually be done.*
Include Security Info as part of Profile	Whether Triggers or Mgmt. Stations are included in the profile.
Rapid Route	Used to configure the iMG for Media Room support. This enhances NAT routing functionality in CPE for better throughput of routed traffic.

TABLE 19-6 Create iMG Internet Profile Security Tab (Continued)

Attribute	Value
Triggers	A set of attributes that allows an application to open a secondary port to transport packets. A trigger opens a secondary port dynamically, and allows you to define the length of time the port can be inactive before it is closed. - Trigger Name - a label that helps identify the trigger. It cannot start with a digit. - Type - protocol for the application, tcp or udp - Start Port - First port in the range for the control session. - End Port - Last port in the range for the control session. - Max. Act. Interval - the amount of time (in milliseconds) the secondary port is allowed to pass traffic before it is closed. The default is 3000 (3 seconds).
Copy values from profile	To create a new profile based on values from an existing profile, select an existing profile from the drop-down list. The fields will pre-populate with the values from the selected profile. Modify any fields as necessary for the new profile.
Create	Creates the profile.
Cancel	Closes the window without creating the profile. The values are not saved.

19.3.2.1 Advanced Trigger Attributes



Trigger Name: test

Secondary Start Port (1024..65535): 1024

Secondary End Port (1024..65535): 65535

Allow Multiple Hosts: Disabled

Session Chaining: Disabled

UDP Session Chaining: Disabled

Binary Address Replacement: Disabled

Address Translation Type: none

FIGURE 19-7 iMG Internet Profile - Security tab - Advanced Trigger Attributes

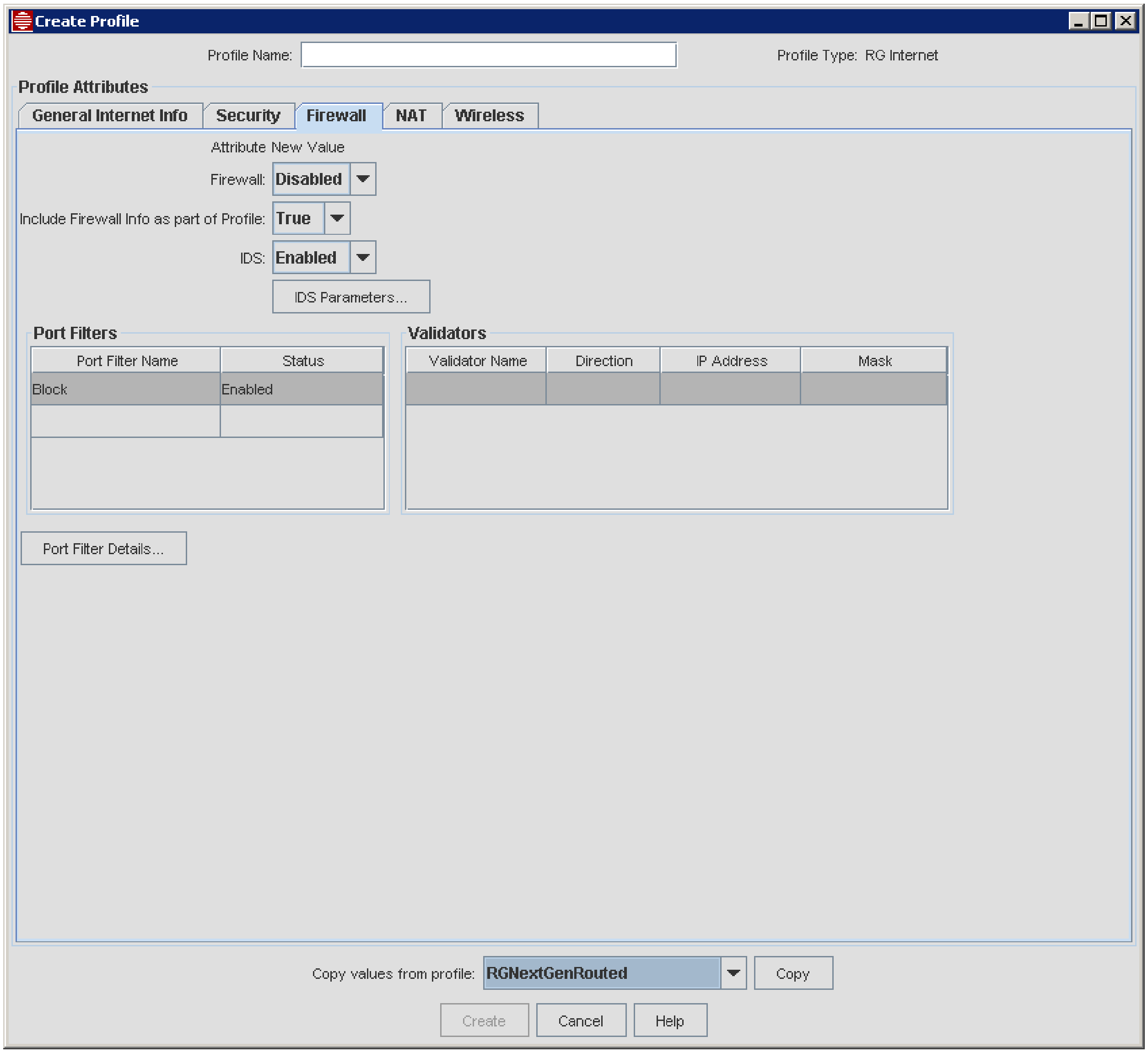
TABLE 19-7 Create iMG Internet Profile Security Tab - Advanced Trigger Attributes

Attribute	Value
Secondary Start Port	The start of the secondary port range for an existing trigger.
Secondary End Port	The end of the secondary port range for an existing trigger.
Allow Multiple Hosts	Controls whether a secondary session can be initiated to/ from same or different remote hosts on the same trigger.
Session Chaining	- Session Chaining - Whether TCP dynamic sessions can also become triggering sessions, which allows multi-level session triggering.
UDP Session Chaining	Whether both UDP and TCP sessions also become triggering sessions, which allows multi-level session triggering.

TABLE 19-7 Create iMG Internet Profile Security Tab - Advanced Trigger Attributes

Attribute	Value
Binary Address Replacement	Enables/disables binary address replacement on an existing trigger. You can then set the type of address replacement (TCP, UDP, both or none)
Address Translation Type	Specifies what type of address replacement is set on a trigger. Incoming packets are searched in order to find their embedded IP address. The address is then replaced by the correct inside host IP address, and NAT translates the packets to the correct destination. You can specify whether you want to carry out address replacement on TCP packets, on UDP packets, or on both TCP and UDP packets.

19.3.3 Firewall Tab



Profile Name:

Profile Type: RG Internet

Firewall: Disabled

Include Firewall Info as part of Profile: True

IDS: Enabled

Port Filter Name	Status
Block	Enabled

Validator Name	Direction	IP Address	Mask

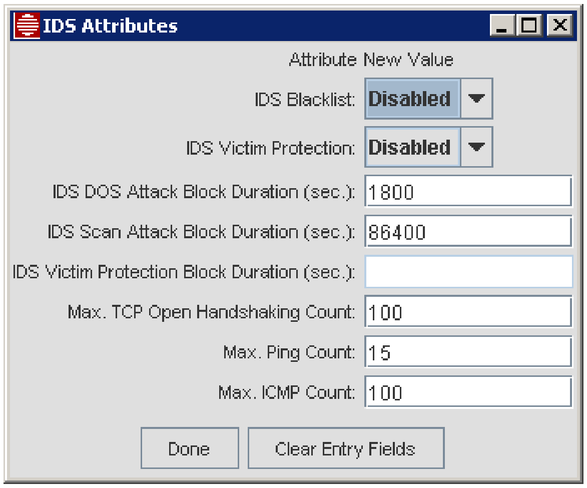
Copy values from profile: RGNextGenRouted

FIGURE 19-8 iMG Internet Profile - Firewall tab

TABLE 19-8 Create iMG Internet Profile Firewall Tab

Attribute	Value
Firewall	Whether the feature is Enabled or Disabled. This option is activated only for Routed Service. Security does not have to be enabled to enter IDS and Port Filters.
Include Firewall Info as part of Profile	Whether IDS and Port Filters are included in the profile. If False, the attributes are configured on the iMG/RG but not activated.
IDS	Whether IDS is Enabled or Disabled. If Enabled, the IDS Parameters window is activated. IDS parameters can be datafilled and enabled regardless of whether the FIrewall feature is enabled, since IDS applies to the iMG, and is not associated with specific Firewall attributes.
Port Filters	Rules that determine what kind of traffic can pass between the external and internal network. - Port Filter Name - A label to help identify the filter. It cannot start with a digit. - Status - Enabled or Disabled
Validators	Blocks the traffic to/from the IP addresses/masks defined. All other traffic is allowed. - Validator Name - A label to help identify the validator. It cannot start with a digit. - Direction - Can be one of the following: - Inbound (Validator blocks incoming traffic based on IP address/mask) - Outbound (Validator blocks outgoing traffic based on IP address/mask) - Both (Validator filters both incoming and outgoing traffic based on IP address/ mask. - IP Address - The IP address to be filtered. - Mask - The mask, such as 255.255.255.0 or 255.255.255.255 (single address)
Copy values from profile	To create a new profile based on values from an existing profile, select an existing profile from the drop-down list. The fields will pre-populate with the values from the selected profile. Modify any fields as necessary for the new profile.
Create	Creates the profile.
Cancel	Closes the window without creating the profile. The values are not saved.

19.3.3.1 IDS Attributes



IDS Blacklist: Disabled

IDS Victim Protection: Disabled

IDS DOS Attack Block Duration (sec.): 1800

IDS Scan Attack Block Duration (sec.): 86400

IDS Victim Protection Block Duration (sec.):

Max. TCP Open Handshaking Count: 100

Max. Ping Count: 15

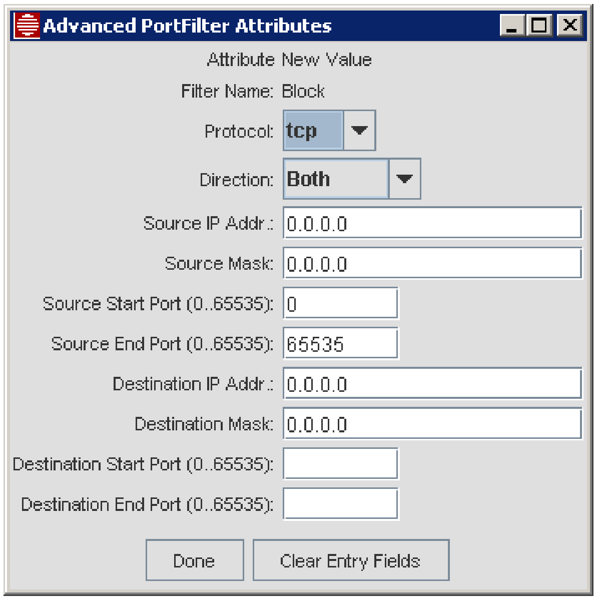
Max. ICMP Count: 100

FIGURE 19-9 iMG Internet Profile - Firewall tab - IDS Attributes

TABLE 19-9 Create iMG Internet Profile Firewall Tab - IDS Attributes

Attribute	Value
IDS Blacklist	Enabled or Disabled - Blacklisting denies an external host access to the system if IDS has detected an intrusion from that host. Access to the network is denied for ten minutes.
IDS Victim Protection	Enabled or Disabled - This protects the system against broadcast pings with a spoofed source address. Packets are blocked for a specified duration (600 minutes by default, can be changed using Duration field below)
IDS DOS Attack Block Duration	A DOS attack is an attempt by an attacker to prevent legitimate users from using a service. If a DOS attack is detected, all suspicious hosts are blocked for a set time limit. Default is 1800 seconds (30 minutes)
IDS Scan Attack Block Duration	If hosts are blocked, sets the duration of the block time limit.
IDS Victim Protection Block Duration	If victim protection is enabled, specifies the duration of the block
Max. TCP Open Handshaking Count	The maximum number of unfinished TCP handshakes allowed before a flood is detected. The attacker is blocked by the time defined in the IDS DOS Attack Block Duration field.
Max. Ping Count	The maximum number of pings allowed before an echo storm is detected. The attacker is blocked by the time defined in the IDS DOS Attack Block Duration field.
Max. ICMP Count	The maximum number of ICMP packets allowed before a flood is detected. The attacker is blocked by the time defined in the IDS DOS Attack Block Duration field.

19.3.3.2 Advanced Port Filter Attributes



Attribute New Value
Filter Name: Block
Protocol: tcp
Direction: Both
Source IP Addr.: 0.0.0.0
Source Mask: 0.0.0.0
Source Start Port (0..65535): 0
Source End Port (0..65535): 65535
Destination IP Addr.: 0.0.0.0
Destination Mask: 0.0.0.0
Destination Start Port (0..65535):
Destination End Port (0..65535):

FIGURE 19-10 iMG Internet Profile - Firewall tab - Port Filter Attributes

TABLE 19-10 Create iMG Internet Profile Firewall Tab - Port Filter Attributes

Attribute	Value
Protocol	udp, tcp, or icmp. For ICMP, there are no Start and Destination Port attributes. Only these three protocols are supported.
Direction	Inbound (allows packets from the external to the internal network), Outbound (allows packets from the internal to the external network) or Both.
Source IP Addr.	The IP address from which packets of the protocol can be sent out. This is used in conjunction with the Source Mask.
Source Mask	The mask for the Source IP Address.
Source Start Port	The start of a source port range for udp or tcp packets.
Source End Port	The end of a source port range for udp or tcp packets.
Destination IP Addr.	The IP address to which packets of the protocol can be sent. This is used in conjunction with the Destination Mask.
Destination Mask	The end of a destination port range for udp or tcp packets.
Destination Start Port	The start of a destination port range for udp or tcp packets.
Destination End Port	The end of a destination port range for udp or tcp packets.

19.3.4 NAT Tab

The NAT tab allows you to set up static IP address and port mappings to the local address space.

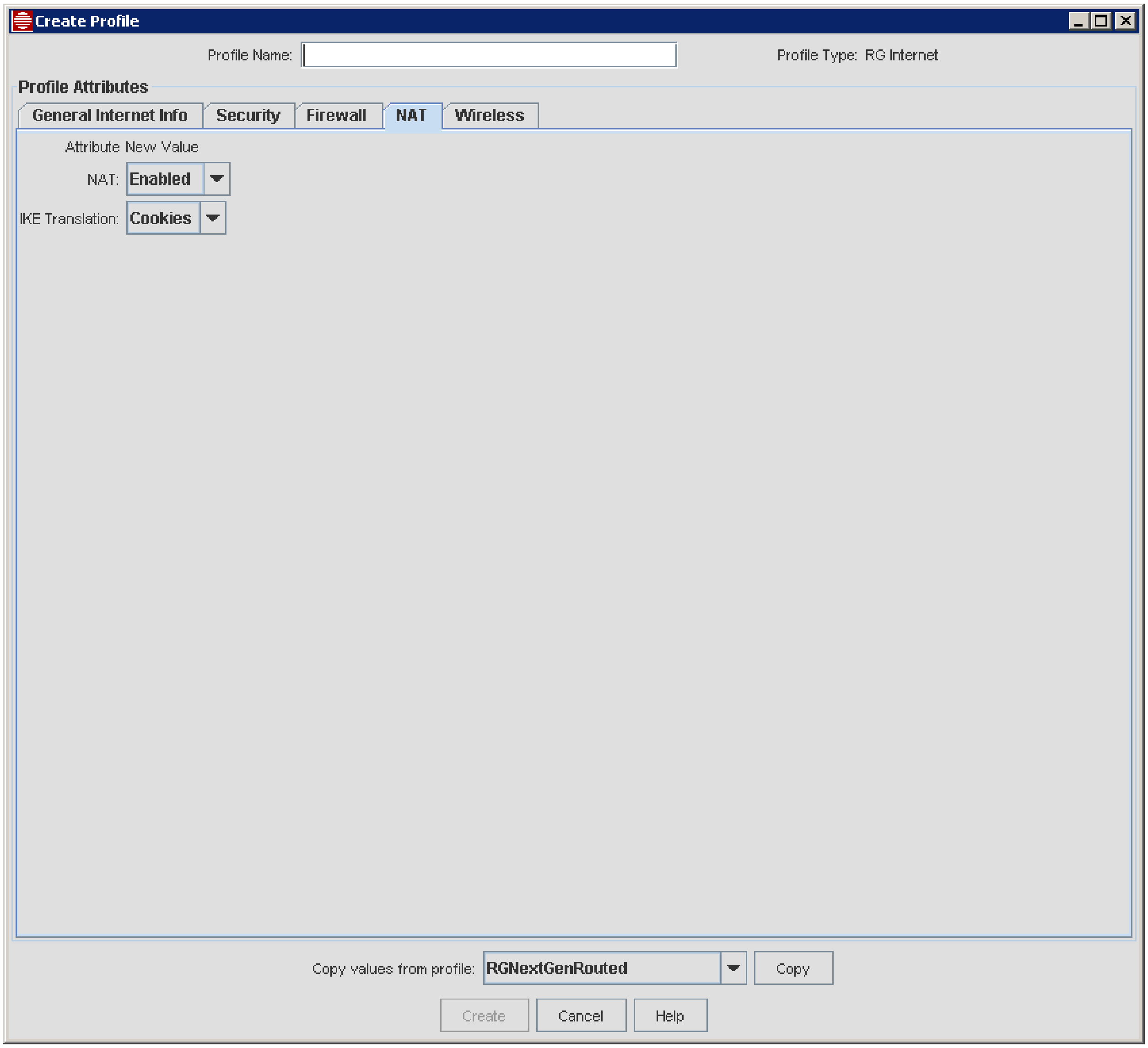


FIGURE 19-11 iMG Internet Profile - NAT tab

TABLE 19-11 Create iMG Internet Profile NAT Tab

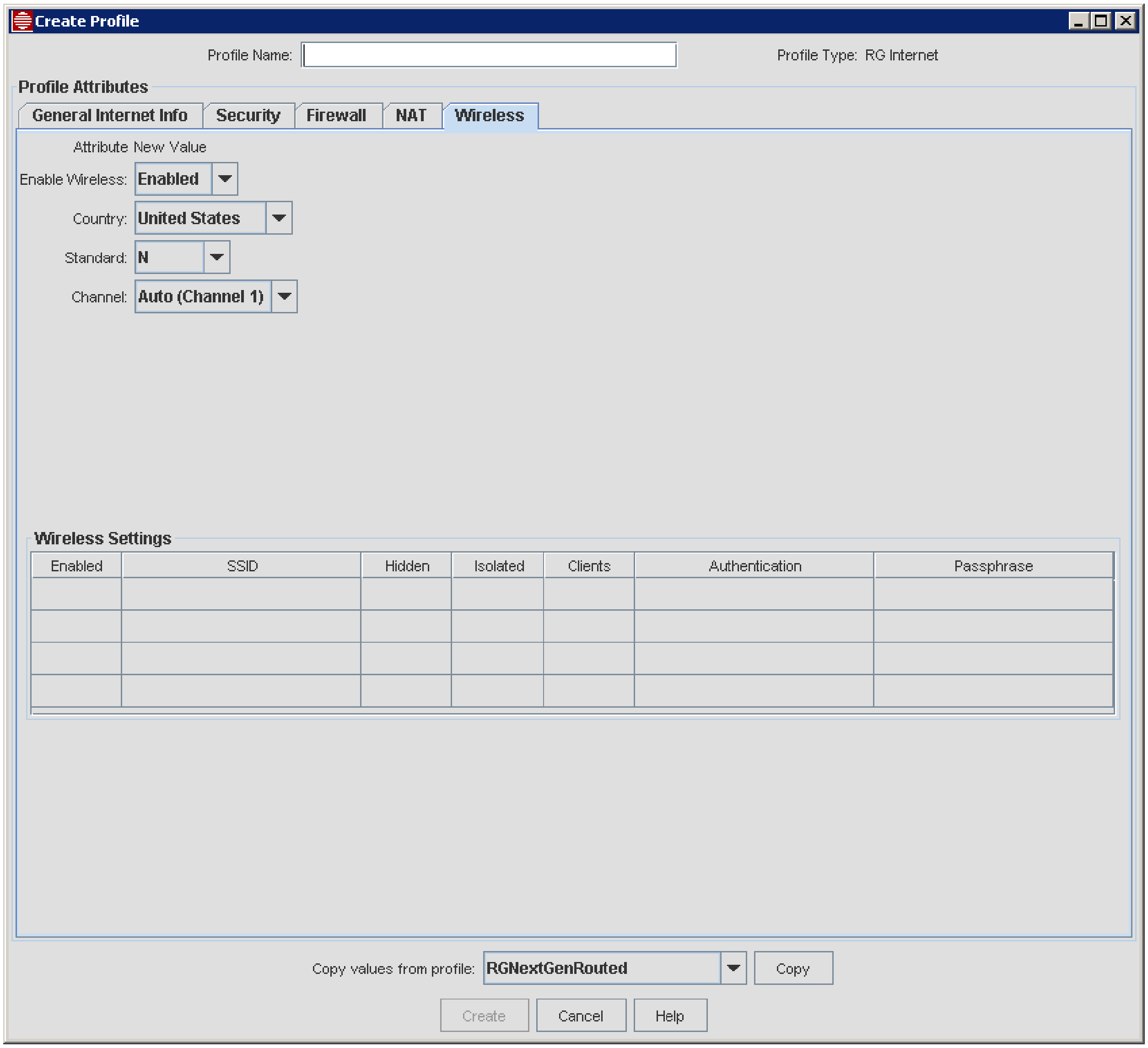
Attribute	Value
NAT	Whether the feature is Enabled or Disabled. This option is activated only for Routed Service.
IKE Translation	Specifies how Internet Key Exchange Packets are translated. - Ports - Source port is translated for IKE packets. - Cookies - IKE cookies are used to identify IKE packets.
Include NAT Info as part of Profile	Whether Global Pools and Reserved Mappings are included in the profile.
Copy values from profile	To create a new profile based on values from an existing profile, select an existing profile from the drop-down list. The fields will pre-populate with the values from the selected profile. Modify any fields as necessary for the new profile.

TABLE 19-11 Create iMG Internet Profile NAT Tab (Continued)

Attribute	Value
Create	Creates the profile.
Cancel	Closes the window without creating the profile. The values are not saved.

19.3.5 Wireless Tab

The Wireless tab in the iMG Internet profile configures wireless settings for iMG 1000 and iMG 2000 series devices. Wireless settings for iMGs running software release 3-x and earlier are configured in the iMG General profile. To configure wireless settings for iMGs running software release 3-x and earlier, see "Wireless Tab" on page 706.



Profile Name:

Profile Type: RG Internet

Enable Wireless: Enabled

Country: United States

Standard: N

Channel: Auto (Channel 1)

Enabled	SSID	Hidden	Isolated	Clients	Authentication	Passphrase

Copy values from profile: RGNextGenRouted

FIGURE 19-12 iMG Internet Profile - Wireless tab

TABLE 19-12 Create iMG Internet Profile Wireless Tab

Attribute	Value
Enable Wireless	Enable or disable the wireless interface on the device. When the wireless network is disabled, the wireless network can be seen but connections are not allowed.
Country	The 802.11d country string for the wireless card.
Standard	Specifies the wireless standard for the device. - B - G - G Only - N - N Only
Channel	The default channel to use. - Auto - Automatically select the best channel when the device starts up. - 1-11 - The specific channel to use.
Wireless Settings	- Enabled - Enables or disables the SSID. - SSID - The SSID for the wireless network. - Hidden - Prevent the SSID from being broadcast. - Disabled - The SSID is broadcast. - Enabled - The SSID is hidden. - Isolated - Specifies whether Client Isolation is implemented in the wireless network. - Enabled - Use Client Isolation in the network. - Disabled - Do not use Client Isolation in the network. - Clients - The maximum number of clients that can connect to the iMG's wireless network. - Authentication - The type of authentication to use in the network. - Open - WPA-PSK - WPA2-PSK - Mixed WPA2/WPA-PSK - Passphrase - The wireless network password.
Copy values from profile	To create a new profile based on values from an existing profile, select an existing profile from the drop-down list. The fields will pre-populate with the values from the selected profile. Modify any fields as necessary for the new profile.
Create	Creates the profile.
Cancel	Closes the window without creating the profile. The values are not saved.

19.4 iMG Video Profile

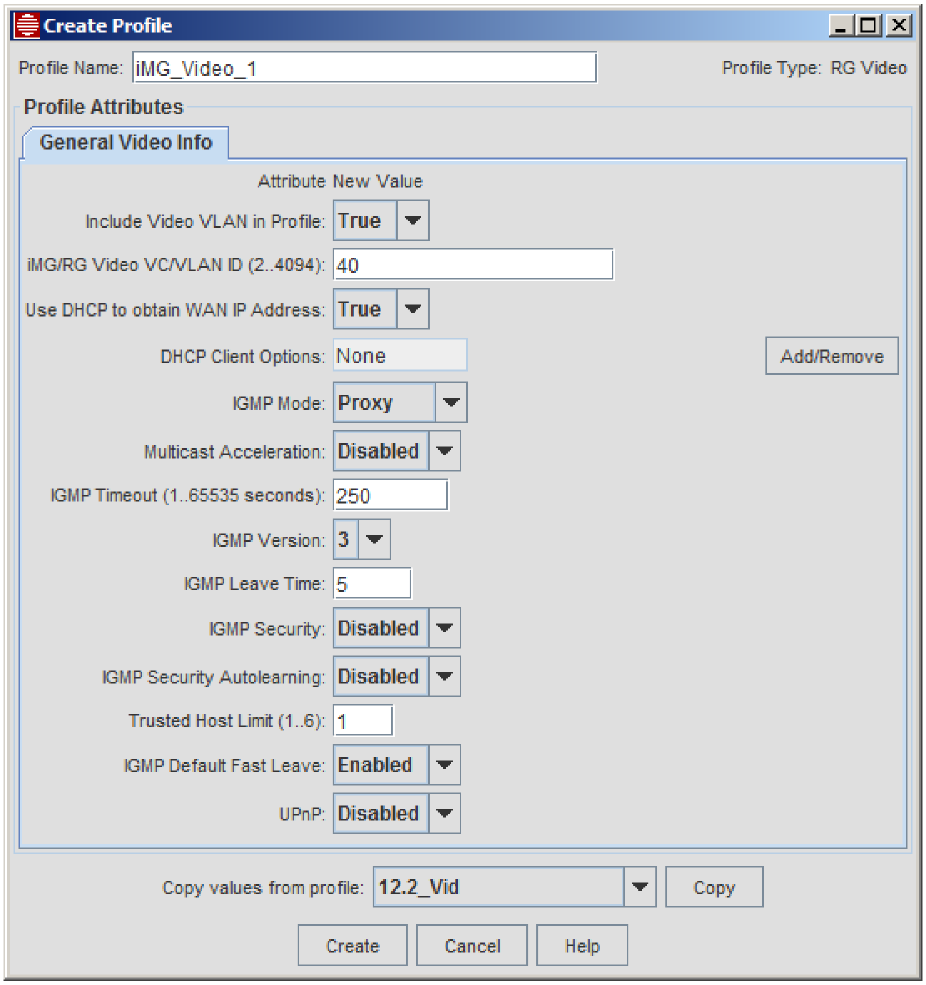
To create a video profile:

1. In the **Network Objects** panel, go to **Network Service Data** > **Profiles**.
2. From the menu, go to **Network Services** > **Profile** > **iMG/RG Service Profiles** > **Create iMG/RG Video Profile**. The **Create Profile** box for the RG Video profile appears.

The video profile contains one tab:

- General Video Info Tab

19.4.1 General Video Info Tab



Create Profile

Profile Name: iMG_Video_1

Profile Type: RG Video

Profile Attributes

General Video Info

Attribute	New Value
Include Video VLAN in Profile:	True
iMG/RG Video VC/VLAN ID (2..4094):	40
Use DHCP to obtain WAN IP Address:	True
DHCP Client Options:	None
IGMP Mode:	Proxy
Multicast Acceleration:	Disabled
IGMP Timeout (1..65535 seconds):	250
IGMP Version:	3
IGMP Leave Time:	5
IGMP Security:	Disabled
IGMP Security Autolearning:	Disabled
Trusted Host Limit (1..6):	1
IGMP Default Fast Leave:	Enabled
UPnP:	Disabled

Copy values from profile: 12.2_Vid

FIGURE 19-13 RG Video Profile

TABLE 19-13 Create RG Video Profile Form

Attribute	Value
Profile Name	A descriptive name that should match the service/function provided Example Names: • Flood - This would match the NONE for IGMP Mode (IGMP Snooping turned off) • Snoop (646 and 656) - Note that all RG600 series RG/IMG will support snooping in the next sw release. • Proxy - The RG performs the IGMP function. Possible Names are: • (These are for ADSL only) • ManualSec2/Proxy (up to two STBs and must specify STN MAC address) • ManualSec3/Proxy (up to three STBs) • AutoSec2/Proxy (up to two STBs and STB sends its MAC address) • AutoSec3/Proxy (up to three STBs) (These will be available in future releases as they are supported.) • ManualSec2/Snoop • ManualSec3/Snoop • AutoSec2/Snoop • AutoSec3/Snoop
Include Video VLAN in Profile	The value entered here depends on the network model: False - The Access Island model is used, and the Internet VLAN Id field is blank. True - The Open Access model is used, and the Internet VLAN Id field is activated.
iMG/RG Video VLAN Id	The VLAN that supports internet service. If the 'Include Video VLAN in Profile' is set to True, this field is activated.
Use DHCP to obtain WAN IP Address	- Used for the Media Room feature.
DHCP Client Options	DHCP client options for the service. Options 3 and 121 are supported. Option 3 is enabled by default in the iMG. Use Add/Remove to open the DHCP Client Options box. You can enable or disable each option listed.
IGMP Mode	None Snooping Proxy
Multicast Acceleration	Used for the Media Room feature.
IGMP Time-out	Number of seconds before channel is dropped because of no IGMP message. The IGMP time-out must be at least 10 seconds greater than the router queries, but not so much higher that it will time-out.
IGMP Version	This field applies to the iMG with version 4-1 and above. Possible values are 1 to 3, with 3 being the default. Refer to the iMG Software Reference Manual.
IGMP Leave Time (0..255)	Time in seconds between when the Leave message form the last host is received and the multicast connection is dropped.

TABLE 19-13 Create RG Video Profile Form (Continued)

Attribute	Value
IGMP Security	Enabled or Disabled When “learning” is enabled the RG will only allow those trusted hosts (STB) if specified in the Triple Play screen to participate in IGMP (ask for broadcast channels When “autolearning” is enabled as well as “learning” the RG when booting up will automatically learn “X” number of trusted hosts (STB) as specified in the video profiles “trusted host limit” field. *Note: IGMP Security, Autolearning, and Trusted Host Limit are currently valid only for ADSL versions of the RG. Release 2.4 will include these features for Ethernet-based iMG/RGs (613, 613, etc.)*
IGMP Security Autolearning	Enabled or Disabled
Trusted Host Limit	Number of hosts (STBs) that the RG can support.
IGMP Default Fast Leave	Enables or Disables the default to keep track of Multicast Group membership by MAC address, so Leaves are processed imme-diately and the interface is removed from the Multicast Group (no timers).
UPnP	Enable or disable UPnP on the iMG. You can enable UPnP for either Internet or video service, but not both simultaneously. If UPnP is enabled on the video service it must be disabled on the Internet service, and vice versa.
Copy values from profile	To create a new profile based on values from an existing profile, select an existing profile from the drop-down list. The fields will pre-populate with the values from the selected profile. Modify any fields as necessary for the new profile.
Create	Creates the profile.
Cancel	Closes the window without creating the profile. The values are not saved.

19.5 iMG Voice Profile

To create a voice profile:

1. In the **Network Objects** panel, go to **Network Service Data** > **Profiles**.
2. From the menu, go to **Network Services** > **Profile** > **iMG/RG Service Profiles** > **Create iMG/RG Voice Profile**. The **Create Profile** box for the RG Voice profile appears.

The voice profile contains one tab:

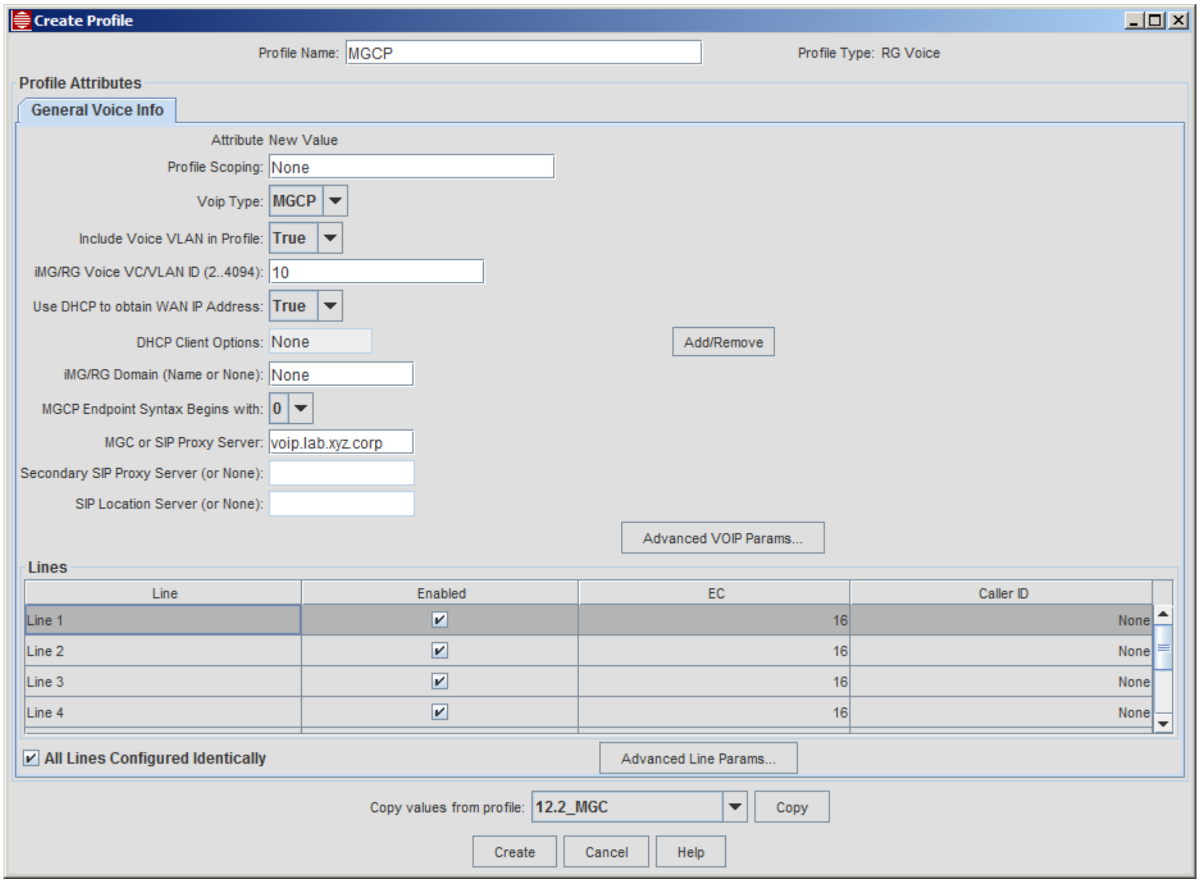
- General Video Info Tab

19.5.1 General Voice Info Tab

Note: With the support of TR-069 iMG and its object model, the values entered in the profile may be shown differently once the iMG is provisioned and queried. (This can occur since a profile is a template that is used to provision the device, and when the device is shown, the device will display its equivalent attributes.) The following table lists the attributes shown in the voice profile and how they may appear when displayed in the service management screen (when using View/Modify Details).

TABLE 19-14 Profile Attributes - Profile and as Provisioned on TR-069 Device

Attribute	TR-069 device	Voice Profile Attribute
Codec (Advanced Line Attributes)	G.711MuLaw G.726 G.711ALaw	g711u g726 g711a
MGCP Profile (Advanced Voip Attributes)	NCS NCS None	Genband NCS (All Else)
DTMF Relay Mode (Advanced Voip Attributes)	Inband RFC2833 SIPInfo	Auto None Out-of-Band



Create Profile

Profile Name: MGCP

Profile Type: RG Voice

Profile Attributes

General Voice Info

Attribute New Value

Profile Scoping: None

Voip Type: MGCP

Include Voice VLAN in Profile: True

iMG/RG Voice VC/VLAN ID (2..4094): 10

Use DHCP to obtain WAN IP Address: True

DHCP Client Options: None

iMG/RG Domain (Name or None): None

MGCP Endpoint Syntax Begins with: 0

MGC or SIP Proxy Server: voip.lab.xyz.corp

Secondary SIP Proxy Server (or None):

SIP Location Server (or None):

Lines

Line	Enabled	EC	Caller ID
Line 1	☑	16	None
Line 2	☑	16	None
Line 3	☑	16	None
Line 4	☑	16	None

☑ All Lines Configured Identically

Copy values from profile: 12.2_MGC

FIGURE 19-14 iMG Voice Profile - General Voice Info Tab

TABLE 19-15 Create iMG/RG Voice Profile Form

Attribute	Value
Profile Name	A descriptive name that should match the service/function provided. The prefix of profile name could include the string that identifies the Access Island as well as the service potential, such as: SPSI-AI01-UpTo4Line The user would give this name to the profile because it would have four voice lines filled in; if the user had one voice line provisioned and needed to provision an additional voice line, the same profile could be used.
Profile Scoping	When used in conjunction with the Triple-Play form, controls the profiles available after selecting the device.port, or controls the device.port available after selecting the Profile.
VOIP Type	The protocol/server configuration to provide VOIP service: - MGCP - SIP Specific types for each are selected in the Advanced VOIP Attributes panel.
Include Voice VLAN in Profile	The value entered here depends on the network model: False - The Access Island model is used, and the Voice VLAN Id field is blank. True - The Open Access model is used, and the Voice VLAN Id field is activated.
iMG/RG Voice VLAN Id	The VLAN that supports voice service. If the 'Include Voice VLAN in Profile' is set to True, this field is activated.
Use DHCP to obtain WAN IP Address	False - Do not use DHCP to obtain the network side address for the iMG. True - Use DHCP to obtain the network side address for the iMG. The default is False.
DHCP Client Options	DHCP client options for the service. Options 3 and 121 are supported. Option 3 is enabled by default in the iMG. Use Add/Remove to open the DHCP Client Options box. You can enable or disable each option listed.
iMG/RG Domain	The critical component of provisioning voice, this is used in the following ways: - the domain that is added to the fully qualified domain name for the voice subnet. Refer to Dynamic DNS Naming for Voice Subnets. - When using MGCP and not using a GenBand device, this can have the VoIP endpoint. The value specified must start with a @. Note that this value must match the endpoint provisioned in the other MGCP device in the configuration. The NMS supplies the "aaln/<telport number>"at the beginning of the string, and then the user continues the value with @. Therefore, values from vendors that do not follow this format are not supported, such as "$MAC:aaln/0@[$IP]". Modifying the end-point syntax is an advanced setting and should not be used unless required by the MGCP server. This value can also be changed on the iMG/RG->Voice Service tab of the service management form. Refer to Changing VoIP Endpoint Syntax.

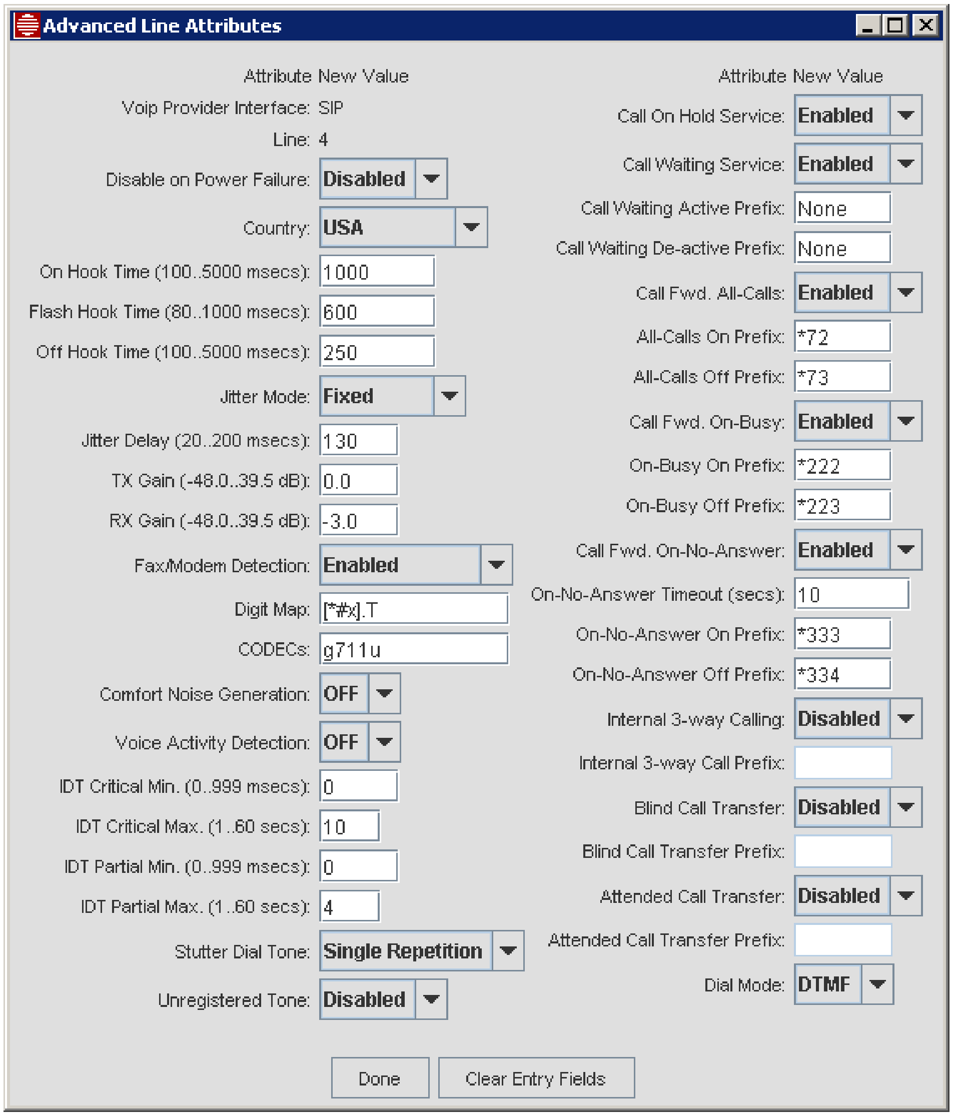
TABLE 19-15 Create iMG/RG Voice Profile Form (Continued)

Attribute	Value
MGCP Endpoint Syntax Begins with	This field applies to iMG 1000 and iMG 2000 series devices. The MGCP call agent uses MGCP endpoint identifiers to address the iMG analog telephone ports. Select '0' or '1' to map the endpoint identifiers to the telephone ports on the iMG sequentially starting with either aaln/0 or aaln/1.
MGC or SIP Proxy Server	Proxy Server for MGCP or SIP
Secondary SIP Proxy Server	This field applies to iMG 1000 and iMG 2000 series devices. A secondary SIP proxy server for redundancy and failover. A secondary proxy server will not function without a primary server.
SIP Location Server	Activated when SIP is chosen as the Voip Type
Advanced VOIP Params	Sets attributes for RTCP (Control parameters for RTP) or SIP. Also includes the type of MGCP/SIP to be used in the profile: iMG/RG MGCP Profile (for example Genband) iMG/RG Admin Profile (for example Sonus) For LCFO, see LCFO. For SIP Subscribe Message Summary, which controls how the iMG receives notifications for events such as Message-Waiting Indication (MWI) from the SIP call server, see SIP Subscribe Message Summary.
Line - Enabled	Activates the other fields, with defaults of EC=8, Caller ID and Call Fwd=None
EC	Echo Cancellation - 0m 8, 16 (default), 32
Caller ID	Appears when SIP is chosen as the type of Voip
SIP Domain	Appears when SIP is chosen as the type of Voip.
All Lines Configured Identically	After choosing one line and its attributes, when the user checks this tic box all other lines will be enabled and have the same attributes.

TABLE 19-15 Create iMG/RG Voice Profile Form (Continued)

Attribute	Value
Advanced Line Params	When at least one line is chosen, this button is active, and the window that appears depends on whether the SIP or MGCP type of profile is being created. Refer to the *Allied Telesis Gateway Product Family Software Reference* for details on all of these attributes. The following parameters are for specific features: • Disable on Power Failure - When the System power Management feature is enabled for a device, this controls that the voice port will be disabled when there is a power failure and the iMG is using a battery. Note that some of the iMGs with 3-8 do not support this feature. This will also appear in the Service management window under the Voice Service tab. Refer to System Power Management. • Fax/Modem Detection - This field will only apply to 3-7 and 3-8 devices that support this feature. For 3-8 devices the option Enhanced is added, when software will determine which mode to select. This will also appear in the Service management window under the Voice Service tab. • Call Waiting Active Prefix - Two fields are added for setting the prefix to use to activate and deactivate call waiting. Since call waiting does not require these prefixes to be set, they are set as a default to 'None' and only used if values (such as *70 to deactivate). This will also appear in the Service management window under the Voice Service tab, but only if the service is SIP and Call Waiting is enabled. • On-No-Answer Timeout (secs) - This is used to calculate the Call forward on-no-answer ring count that is used on the iMG. The number of seconds is divided by 3 to get the ring count. The timeout in seconds that appears on the device details form (from the Voice Service tab) is calculated by multiplying the ring cadence by 3, and so may be different than what is in the profile. Note: The attributes already have defaults filled in, and should not be changed unless for a specific reason. If the user tries to change these values and these are not allowed, the change will fail, and the user must look in the console file to review recent commands to find the failure (webserver: Conflict failure).
Copy values from profile	To create a new profile based on values from an existing profile, select an existing profile from the drop-down list. The fields will pre-populate with the values from the selected profile. Modify any fields as necessary for the new profile.
Create	Creates the profile.
Cancel	Closes the window without creating the profile. The values are not saved.

19.5.1.1 Advanced Line Attributes



Advanced Line Attributes

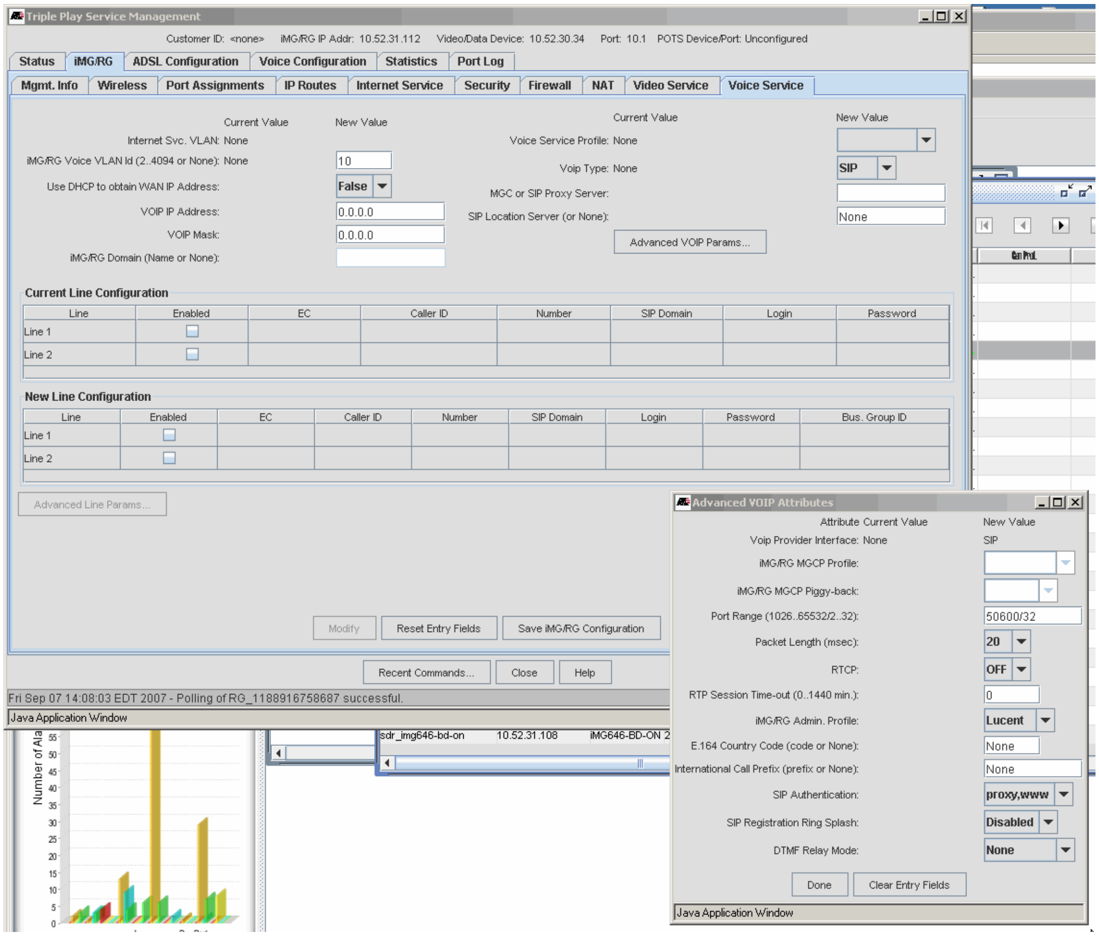
Attribute	New Value
Voip Provider Interface:	SIP
Line:	4
Disable on Power Failure:	Disabled
Country:	USA
On Hook Time (100..5000 msecs):	1000
Flash Hook Time (80..1000 msecs):	600
Off Hook Time (100..5000 msecs):	250
Jitter Mode:	Fixed
Jitter Delay (20..200 msecs):	130
TX Gain (-48.0..39.5 dB):	0.0
RX Gain (-48.0..39.5 dB):	-3.0
Fax/Modem Detection:	Enabled
Digit Map:	[*#x].T
CODECs:	g711u
Comfort Noise Generation:	OFF
Voice Activity Detection:	OFF
IDT Critical Min. (0..999 msecs):	0
IDT Critical Max. (1..60 secs):	10
IDT Partial Min. (0..999 msecs):	0
IDT Partial Max. (1..60 secs):	4
Stutter Dial Tone:	Single Repetition
Unregistered Tone:	Disabled

Attribute	New Value
Call On Hold Service:	Enabled
Call Waiting Service:	Enabled
Call Waiting Active Prefix:	None
Call Waiting De-active Prefix:	None
Call Fwd. All-Calls:	Enabled
All-Calls On Prefix:	*72
All-Calls Off Prefix:	*73
Call Fwd. On-Busy:	Enabled
On-Busy On Prefix:	*222
On-Busy Off Prefix:	*223
Call Fwd. On-No-Answer:	Enabled
On-No-Answer Timeout (secs):	10
On-No-Answer On Prefix:	*333
On-No-Answer Off Prefix:	*334
Internal 3-way Calling:	Disabled
Internal 3-way Call Prefix:	
Blind Call Transfer:	Disabled
Blind Call Transfer Prefix:	
Attended Call Transfer:	Disabled
Attended Call Transfer Prefix:	
Dial Mode:	DTMF

FIGURE 19-15 Advanced Line Attributes - SIP

19.5.2 Business Group ID for SIP

The concept the Business Group ID for SIP is specific to Lucent and Sonus. To configure this ID, access the *iMG/RG -> Voice Service* Tab. If the user chooses the Voip Type as SIP, and then under Advanced VOIP Attributes chooses the iMG/RG Admin. Profile as Lucent or Sonus and clicks on Done, the New Line Configuration table will now include the Bus. Group ID. Refer to the following figure.



Customer ID: <none> iMG/RG IP Addr: 10.52.31.112 Video/Data Device: 10.52.30.34 Port: 10.1 POTS Device/Port: Unconfigured

	Current Value	New Value
Internet Svc. VLAN:	None	
iMG/RG Voice VLAN Id (2..4094 or None):	None	10
Use DHCP to obtain WAN IP Address:		False
VOIP IP Address:		0.0.0.0
VOIP Mask:		0.0.0.0
iMG/RG Domain (Name or None):		

	Current Value	New Value
Voice Service Profile:	None	
Voip Type:	None	SIP
MGC or SIP Proxy Server:		
SIP Location Server (or None):		None

Current Line Configuration

Line	Enabled	EC	Caller ID	Number	SIP Domain	Login	Password
Line 1	□						
Line 2	□						

New Line Configuration

Line	Enabled	EC	Caller ID	Number	SIP Domain	Login	Password	Bus. Group ID
Line 1	□							
Line 2	□							

Fri Sep 07 14:08:03 EDT 2007 - Polling of RG_1188916758687 successful.

sdr_img646-bd-on 10.52.31.108 iMG646-BD-ON 2

Attribute	Current Value	New Value
Voip Provider Interface:	None	SIP
iMG/RG MGCP Profile:		
iMG/RG MGCP Piggy-back:		
Port Range (1026..65532/2..32):		50600/32
Packet Length (msec):		20
RTCP:		OFF
RTP Session Time-out (0..1440 min.):		0
iMG/RG Admin. Profile:		Lucent
E.164 Country Code (code or None):		None
International Call Prefix (prefix or None):		None
SIP Authentication:		proxy,www
SIP Registration Ring Splash:		Disabled
DTMF Relay Mode:		None

FIGURE 19-16 Setting the Business Group ID for SIP (Lucent of SONUS)

Note: *If there is a SIP Voice Profile for SIP, with type Lucent of Sonus, the user could also choose a Voice Service Profile that matched (such as Profile SIP_SONUS), and the Bus. Group ID field would appear after selecting another tab and then re-selecting Voice Service to refresh the page.*

20. Basic Configurations with Sample Profiles

The following descriptions isolate each service. In most cases services are bundled, but describing each service and its specific Profile(s) allows key fields/values to be highlighted.

TABLE 20-1 Profile Set for Access Island 1

Service	Profile Types and Names	Description and Figure Reference
Customer Interface (iMAP)	7Mbps 11Mbps 15Mbps 100Mbps	Profile Name matches the speed required ADSL (1 STB and 3Mbps for data) ADSL (2 STB and 3Mbps for data) ADSL (3 STB and 3Mbps for data) Ethernet
Transparent LAN Service (TLS)	RG General="Business_A"	Transparent LAN Service (TLS)
Data (Internet)		
- Bridged	RG General= "DVLKND-AI01-1T_11_2V" Internet ="Bridged Int Srv"	Internet - Bridged
- Routed	RG General= "DVLKND-AI01-1T_11_2V" Internet= "Routed Int Srv"	Internet - Routed
- Routed - NAT	RG General= "DVLKND-AI01-1T_11_2V" Internet="NAT Int Srv"	Internet - Routed - NAT
Video		
- Snooping	RG General= "Video_only" Video="Snooping"	Video - Snooping

- Proxy	RG General= "Video_only"
	Video="Flood"
	Video="Snoop"
	Video="Proxy"
		Video - Proxy

Voice		
- MGCP		
- GBG6	RG General= "Voice_only" Voice="RG-POTS-4Line"	Voice - Public and Private
- Nuera		Future
- ATI		Future
- SIP		
- SIP	Voice="RG-POTS-4Line"	
- SIP - SONUS		Future

The following subsections include a figure that includes the main components involved in each type of RG service and their variants. Example profiles are then shown so that the user can understand the relationship between the service type and the values that are data filled in the profile.

20.1 Transparent LAN Service (TLS)

Most commonly, TLS is used to join two sites (usually of a business) through the upstream switches of the RGs. This is an Ethernet transport service, at layer 2. Note that data must be untagged. Refer to Figure 20-1.

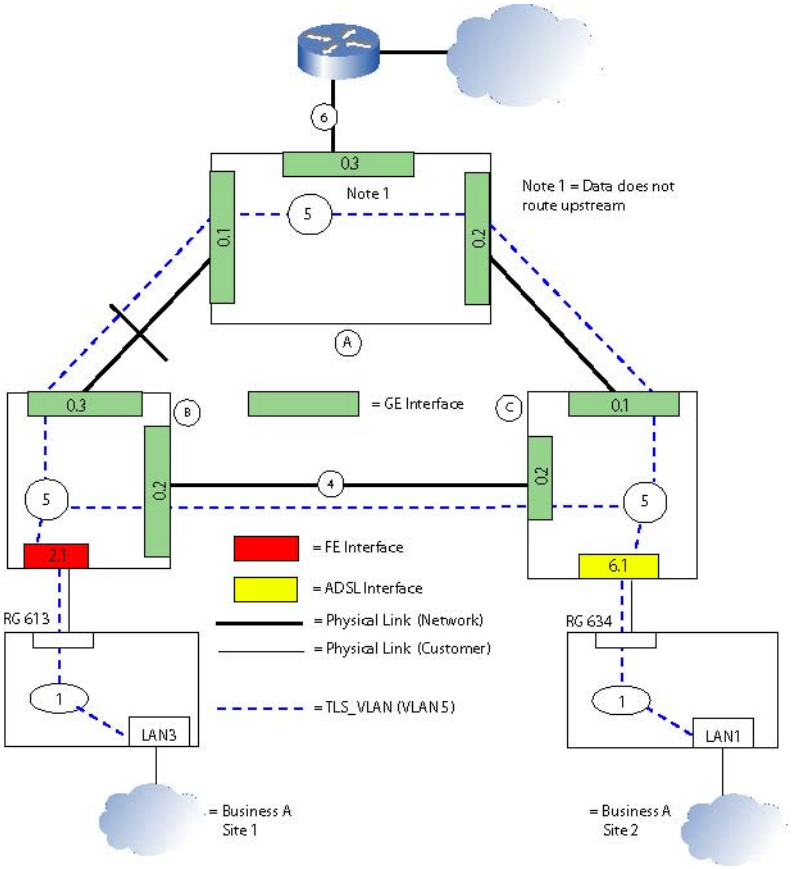


FIGURE 20-1 TLS Configuration

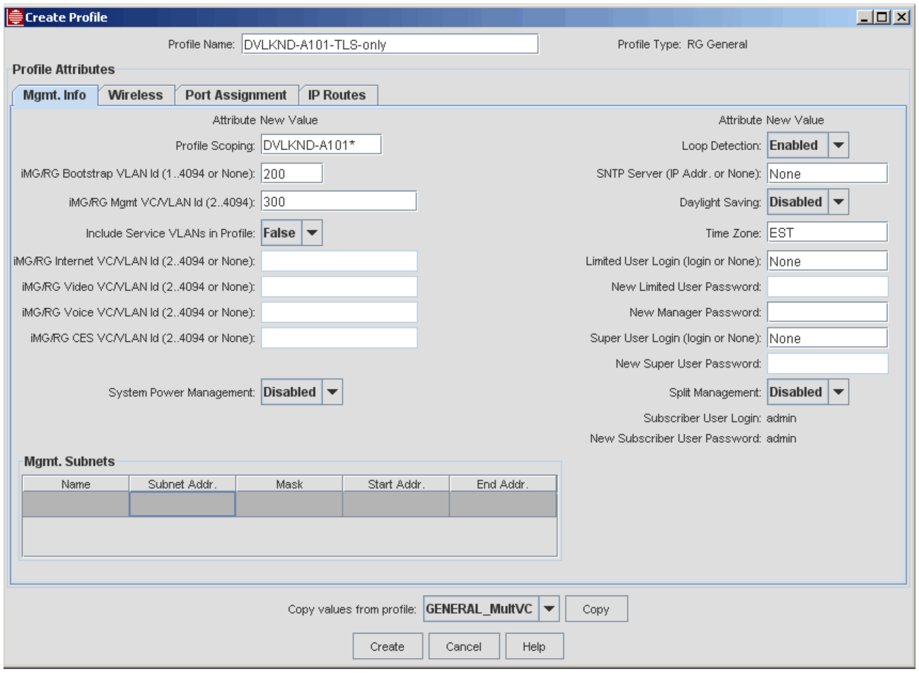
The following screen examples show the sample profiles included with the NMS and what they contain.

TABLE 20-2 Example Profiles for TLS

Profile Type	Example Profile Name	Description and Figure Reference
RG General Profile	DVLKND-AI01-TLS-only	In Mgmt. Info tab, no service VLANs are filled in. Can set Limited and Super User ID and password. Can set password only for Manager password. Port Assignment tab has only one port filled, as TLS. No IP routes required, but there should be a route to a back office management subnet.
RG Internet Profile	N/A	None (default)

TABLE 20-2 Example Profiles for TLS

Profile Type	Example Profile Name	Description and Figure Reference
RG Video Profile	N/A	None (default)
RG Voice Profile	N/A	None (default)



Profile Name: DVLKND-A101-TLS-only

Profile Type: RG General

Profile Attributes

Attribute New Value

Profile Scoping: DVLKND-A101*

iMG/RG Bootstrap VLAN Id (1..4094 or None): 200

iMG/RG Mgmt VC/VLAN Id (2..4094): 300

Include Service VLANs in Profile: False

iMG/RG Internet VC/VLAN Id (2..4094 or None):

iMG/RG Video VC/VLAN Id (2..4094 or None):

iMG/RG Voice VC/VLAN Id (2..4094 or None):

iMG/RG CES VC/VLAN Id (2..4094 or None):

System Power Management: Disabled

Attribute New Value

Loop Detection: Enabled

SNTP Server (IP Addr. or None): None

Daylight Saving: Disabled

Time Zone: EST

Limited User Login (login or None): None

New Limited User Password:

New Manager Password:

Super User Login (login or None): None

New Super User Password:

Split Management: Disabled

Subscriber User Login: admin

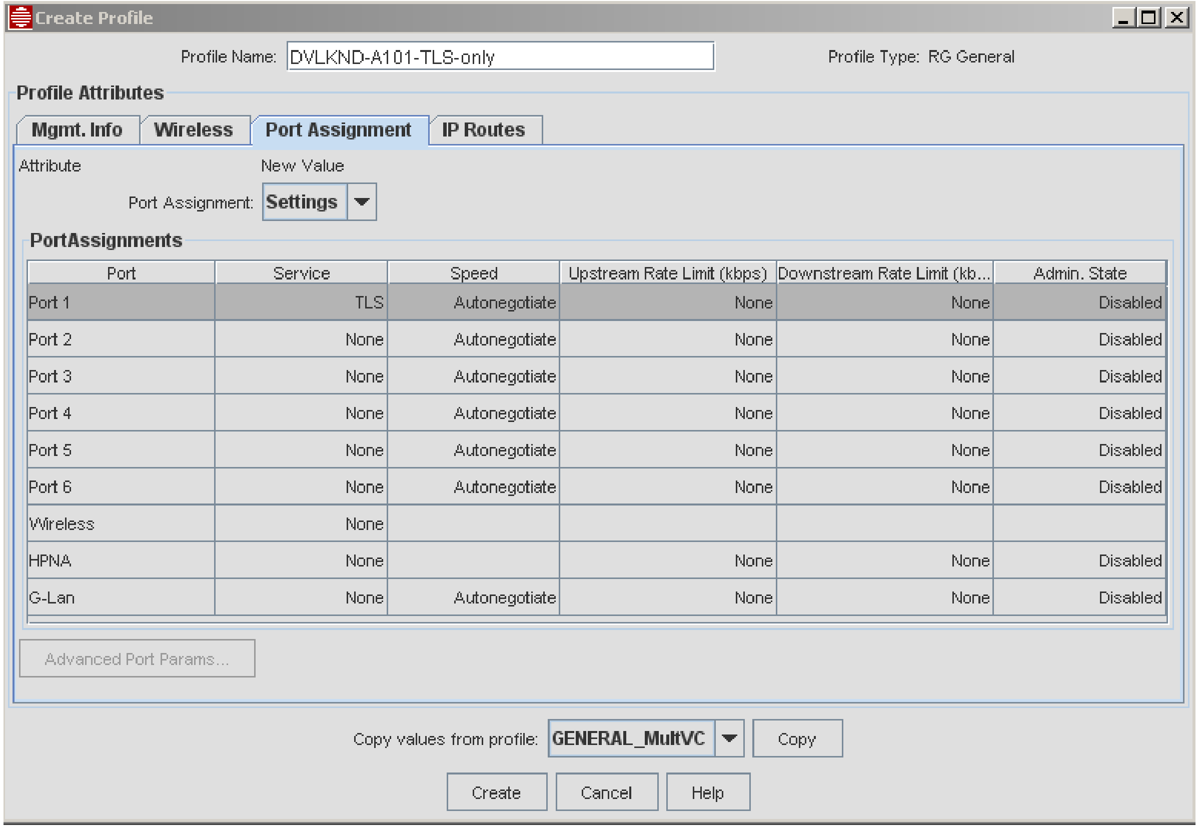
New Subscriber User Password: admin

Mgmt. Subnets

Name	Subnet Addr.	Mask	Start Addr.	End Addr.

Copy values from profile: GENERAL_MultVC

FIGURE 20-2 RG General Profile for TLS - Mgmt Info Tab



Profile Name: DVLKND-A101-TLS-only

Profile Type: RG General

Profile Attributes

Attribute	New Value
Port Assignment:	Settings

PortAssignments

Port	Service	Speed	Upstream Rate Limit (kbps)	Downstream Rate Limit (kb...	Admin. State
Port 1	TLS	Autonegotiate	None	None	Disabled
Port 2	None	Autonegotiate	None	None	Disabled
Port 3	None	Autonegotiate	None	None	Disabled
Port 4	None	Autonegotiate	None	None	Disabled
Port 5	None	Autonegotiate	None	None	Disabled
Port 6	None	Autonegotiate	None	None	Disabled
Wireless	None				
HPNA	None		None	None	Disabled
G-Lan	None	Autonegotiate	None	None	Disabled

Copy values from profile: GENERAL_MultVC

FIGURE 20-3 RG General Profile for TLS - Port Assignment Tab

20.2 Internet - Bridged

In Internet - Bridged service, a data device (such as a PC) connects with the ISP on the same VLAN, so there is no routing. In essence, the RG is like one end of a TLS connection. Refer to Figure 20-4.

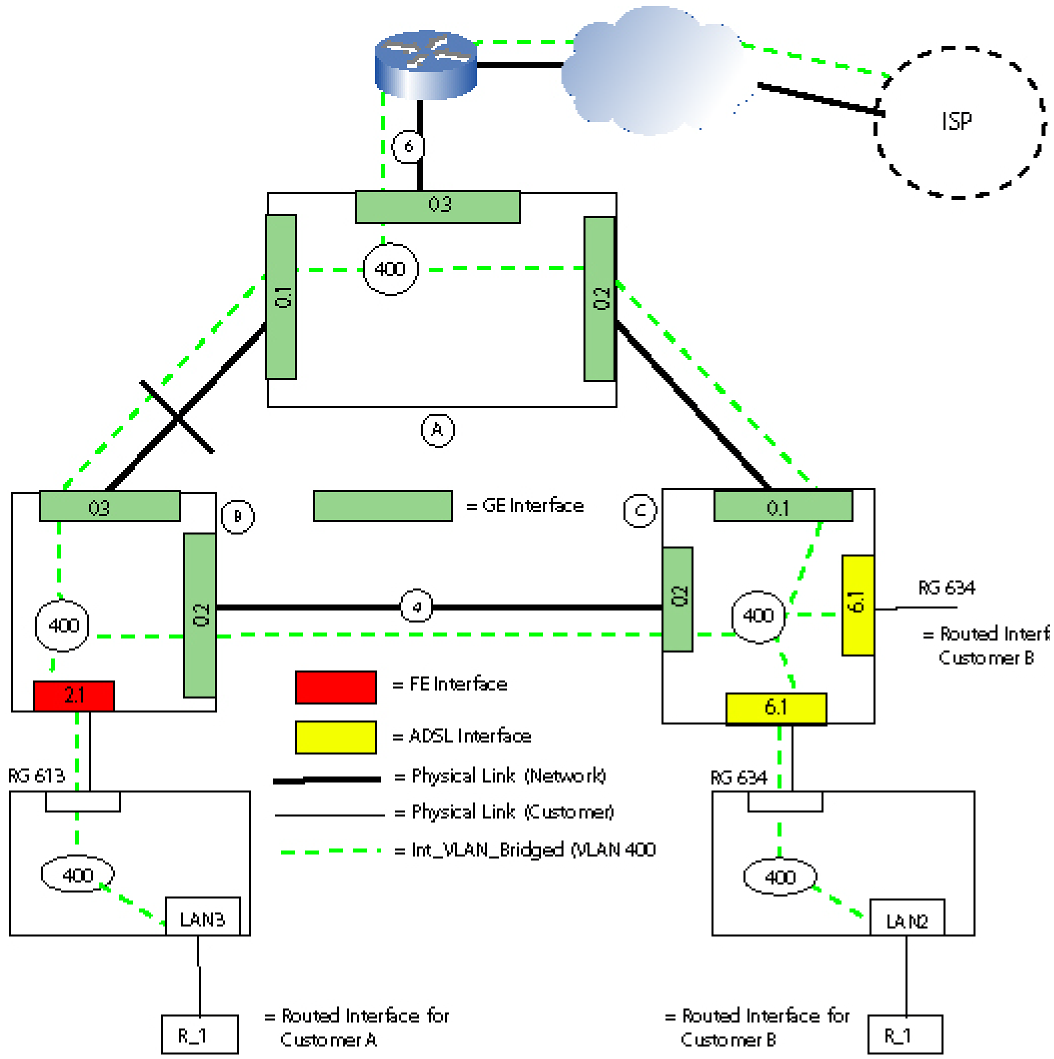
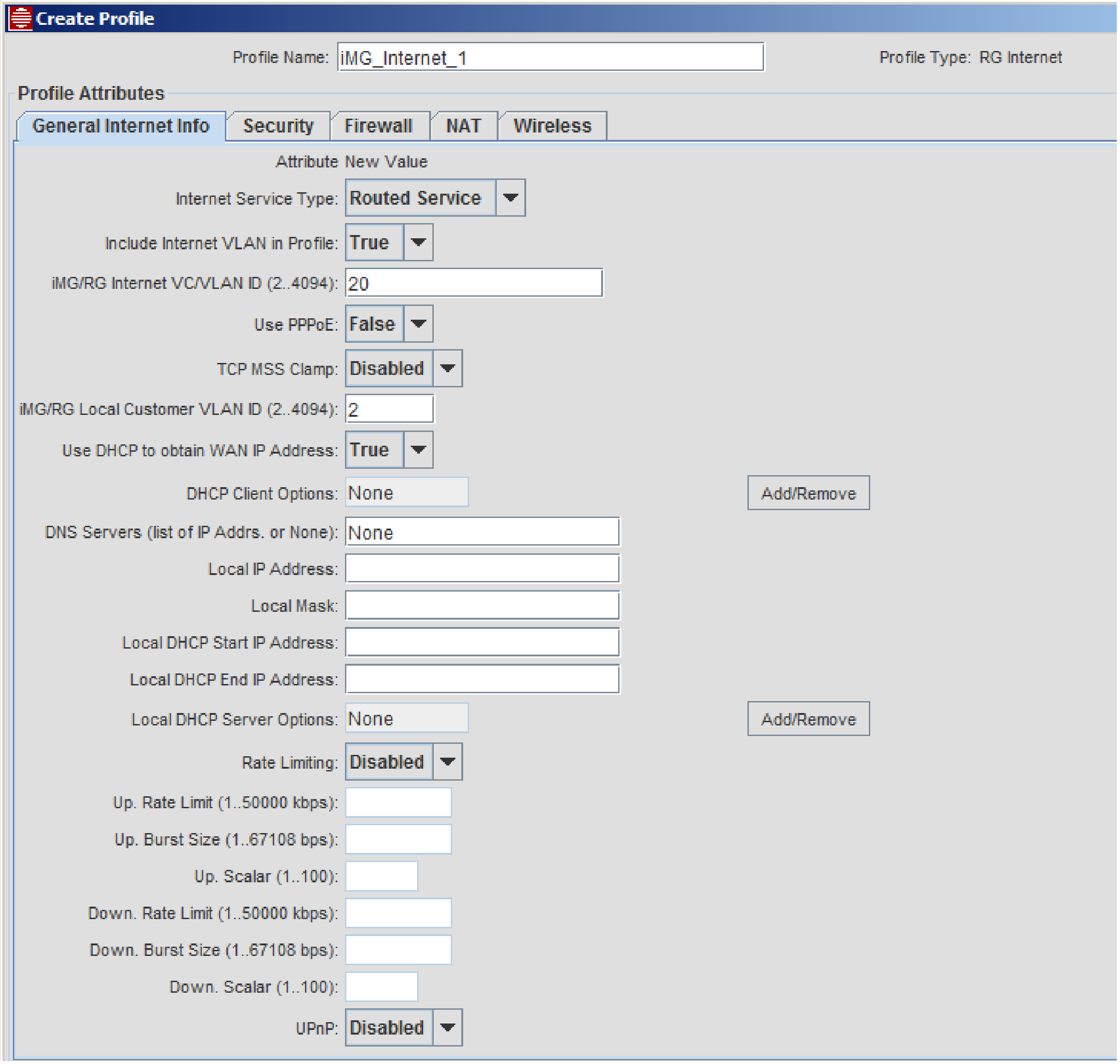


FIGURE 20-4 Internet - Bridged Configuration

The following table lists the sample profiles included with the NMS and what they contain.

TABLE 20-3 Example Profiles for Internet - Bridged

Profile Type	Example Profile Name	Description
RG General Profile	“Internet_only_bridged”	In Mgmt. Info tab, Internet VLAN (400) filled in. Port Assignment tab has only one port filled, as Internet No IP Routes used
RG Internet	“Bridged Service”	Internet Service Type is Bridged Service No iMG/RG Local Customer VLAN



Create Profile

Profile Name: iMG_Internet_1

Profile Type: RG Internet

Profile Attributes

Attribute	New Value
Internet Service Type:	Routed Service
Include Internet VLAN in Profile:	True
iMG/RG Internet VC/VLAN ID (2..4094):	20
Use PPPoE:	False
TCP MSS Clamp:	Disabled
iMG/RG Local Customer VLAN ID (2..4094):	2
Use DHCP to obtain WAN IP Address:	True
DHCP Client Options:	None
DNS Servers (list of IP Addrs. or None):	None
Local IP Address:	
Local Mask:	
Local DHCP Start IP Address:	
Local DHCP End IP Address:	
Local DHCP Server Options:	None
Rate Limiting:	Disabled
Up. Rate Limit (1..50000 kbps):	
Up. Burst Size (1..67108 bps):	
Up. Scalar (1..100):	
Down. Rate Limit (1..50000 kbps):	
Down. Burst Size (1..67108 bps):	
Down. Scalar (1..100):	
UPnP:	Disabled

FIGURE 20-5 Internet Bridged Service - Profile “Bridged Service”

20.3 Internet - Routed

In Internet - Routed service, the RG has a routing function; there are two VLANs, one local to the RG and one for transport to the ISP. The RG IP address is included in packets from the data device. The DHCP function on the LAN side of the RG is included in the Triple Play form. Refer to Figure 20-6.

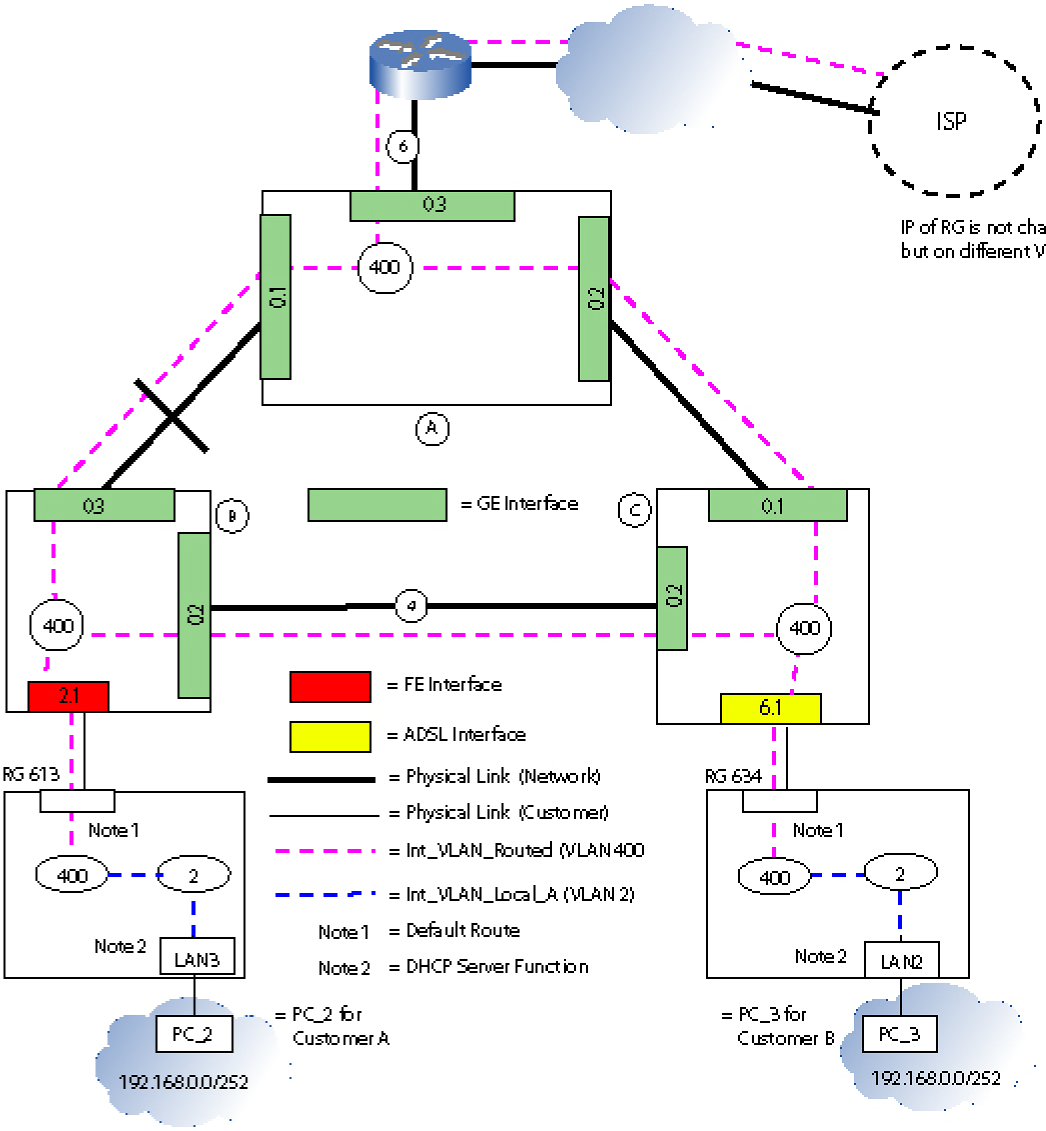
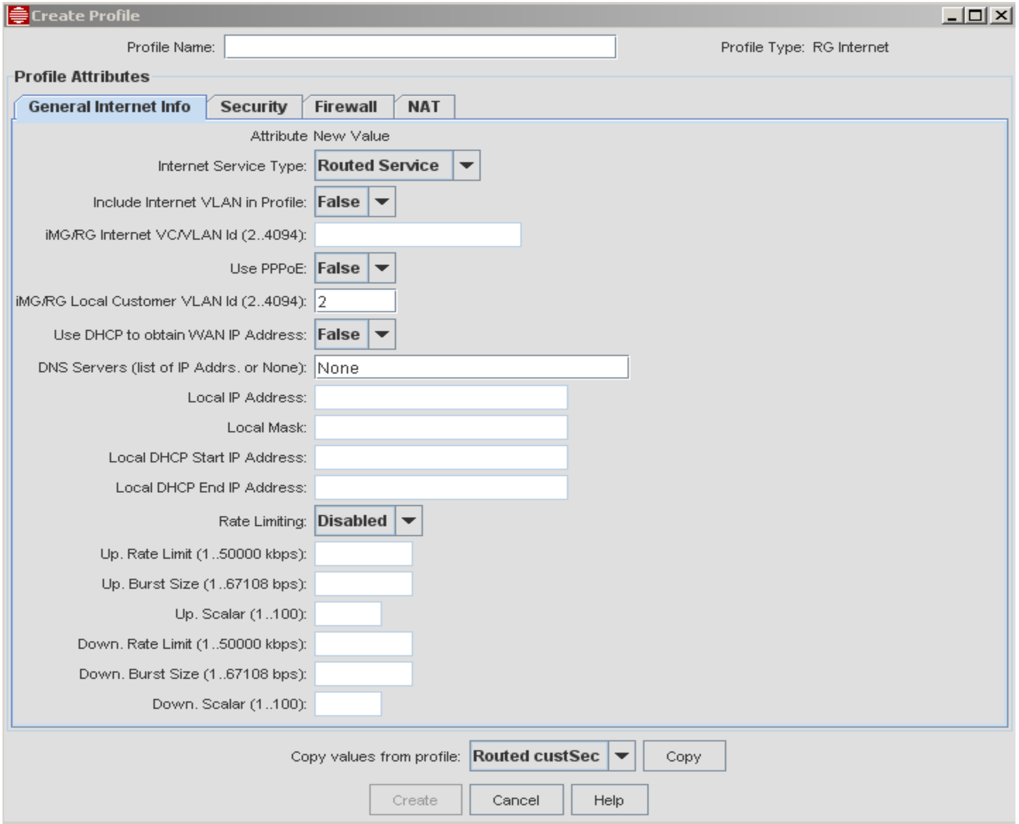


FIGURE 20-6 Internet - Routed Configuration

The following table lists the sample profiles included with the AlliedView NMS and what they contain.

TABLE 20-4 Example Profiles for Internet - Routed

Profile Type	Example Profile Name	Description
RG General Profile	“Internet_Routed_or_NAT”	In Mgmt. Info tab, Internet VLAN (400) filled in. Port Assignment tab has only one port filled, as Internet No IP routes used
RG Internet	“RoutedService”	Internet Service Type is Routed Service Need iMG/RG Local Customer VLAN - This must not be a VLAN also used to deliver services to the WAN port. DNS Servers - This will be used (take priority) only when DNS servers are not identified in the DHCP offer. Firewall should be disabled.



Profile Name:

Profile Type: RG Internet

Attribute New Value

Internet Service Type: Routed Service

Include Internet VLAN in Profile: False

iMG/RG Internet VC/VLAN Id (2..4094):

Use PPPoE: False

iMG/RG Local Customer VLAN Id (2..4094): 2

Use DHCP to obtain WAN IP Address: False

DNS Servers (list of IP Addrs. or None): None

Local IP Address:

Local Mask:

Local DHCP Start IP Address:

Local DHCP End IP Address:

Rate Limiting: Disabled

Up. Rate Limit (1..50000 kbps):

Up. Burst Size (1..67108 bps):

Up. Scalar (1..100):

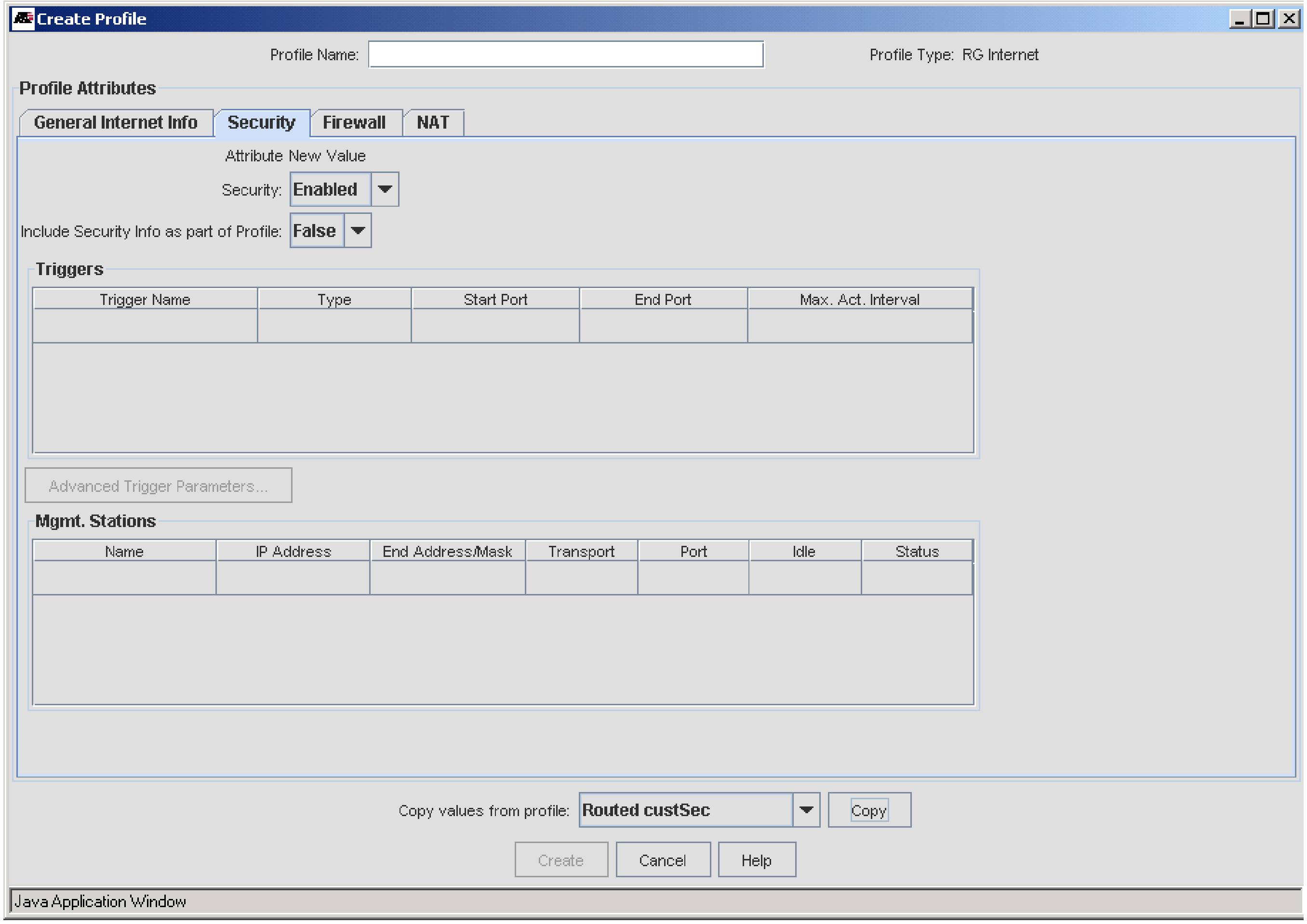
Down. Rate Limit (1..50000 kbps):

Down. Burst Size (1..67108 bps):

Down. Scalar (1..100):

Copy values from profile: Routed custSec

FIGURE 20-7 Internet Routed Service - Profile “Routed custSec” - General Tab



Profile Name:

Profile Type: RG Internet

Attribute	New Value
Security:	Enabled
Include Security Info as part of Profile:	False

Trigger Name	Type	Start Port	End Port	Max. Act. Interval

Name	IP Address	End Address/Mask	Transport	Port	Idle	Status

Copy values from profile: Routed custSec

FIGURE 20-8 Internet Routed Service - Profile “Routed custSec” - Security Tab

20.4 Internet - Routed - NAT

An Internet - Routed NAT service is similar to the Routed service, with the key difference that IP numbering is local; the ISP sends packets to an RG IP address that is defined on a VLAN that is not local to the RG. A local VLAN is defined for the local IP numbering. Refer to Figure 20-9.

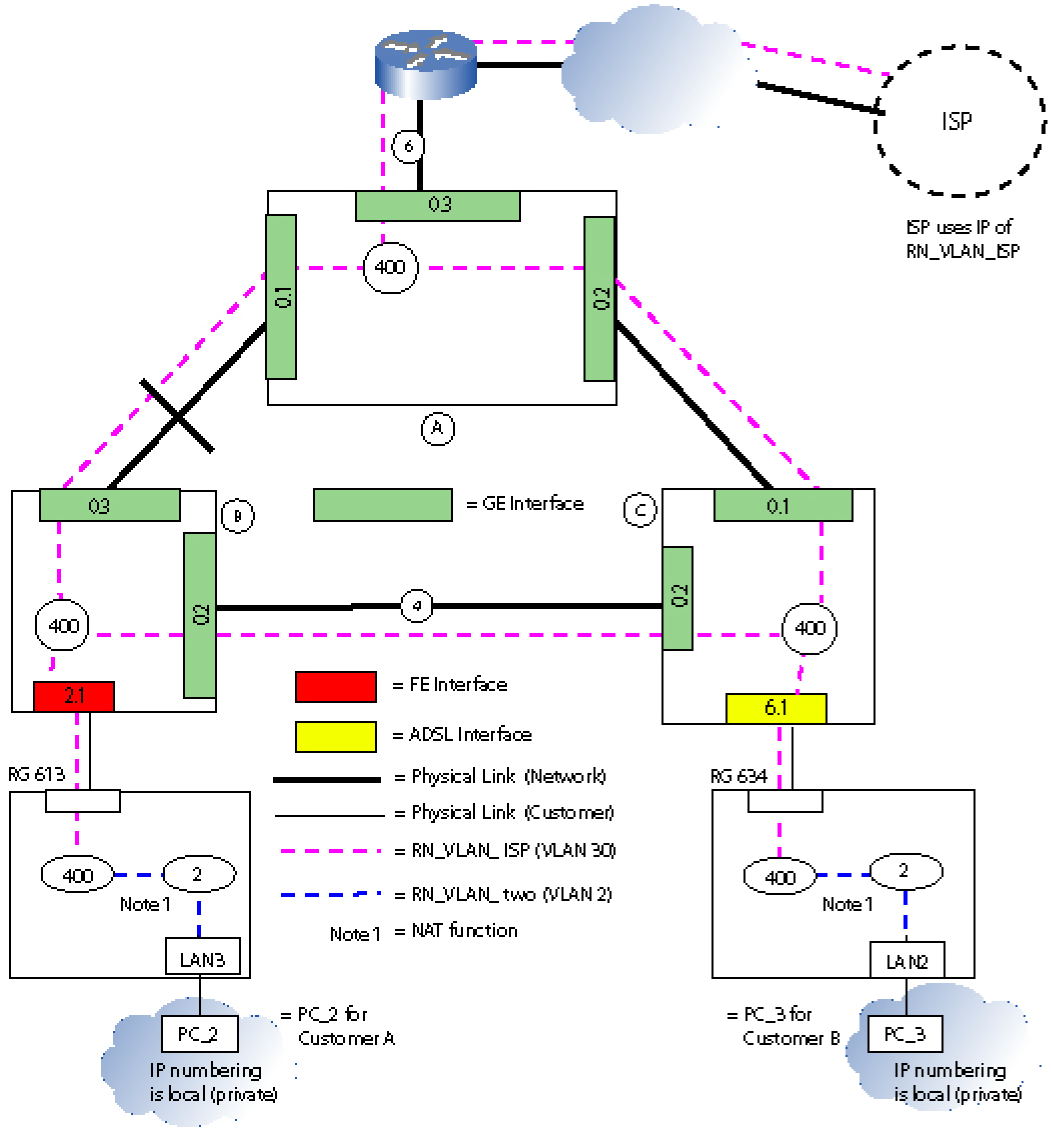
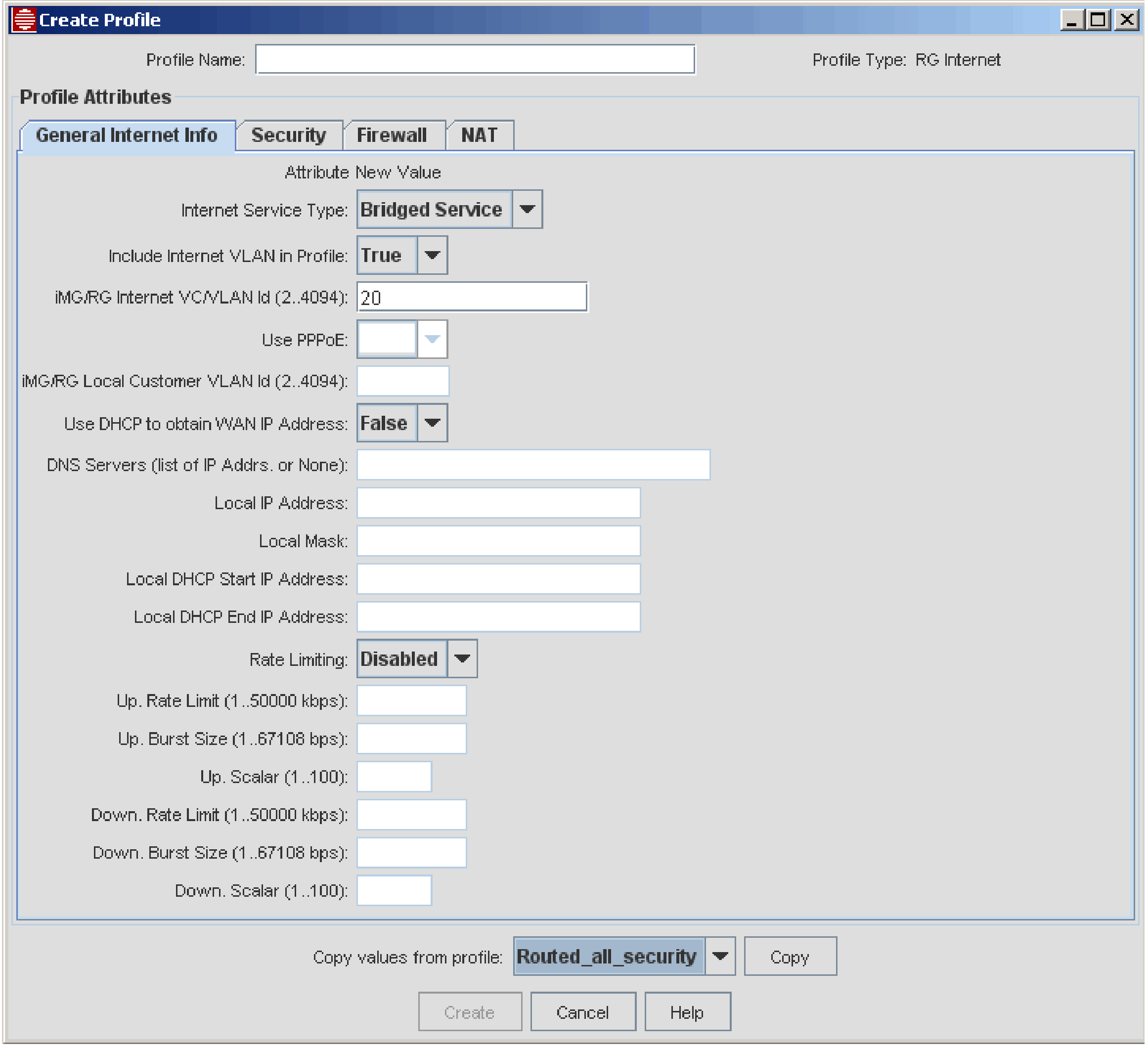


FIGURE 20-9 Internet - Routed NAT Configuration

The following table lists the sample profiles included with the NMS and what they contain.

TABLE 20-5 Example Profiles for Internet - Routed - NAT

Profile Type	Example Profile Name	Description
RG General Profile	"Internet_Routed_or_NAT"	In Mgmt. Info tab, Internet VLAN (400) filled in. Port Assignment tab has only one port filled, as Internet No IP routes used
Routed Service NAT	"Routed/all security"	General Internet Info Tab - Internet Service Type is Routed Service - Need iMG/RG Local Customer VLAN Security Tab - Security Enabled - Security Info as part of Profile is True - Triggers and Mgmt. Stations set



Profile Name:

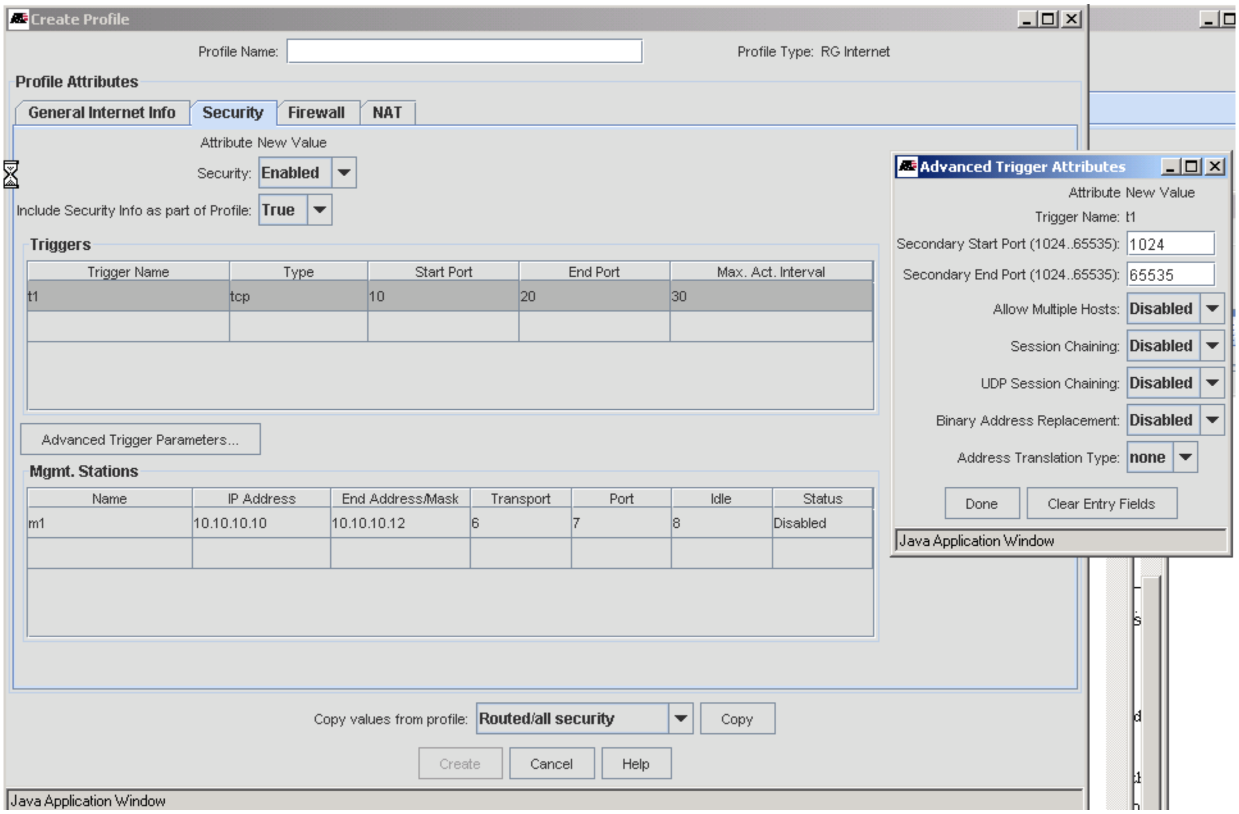
Profile Type: RG Internet

Profile Attributes

Attribute	New Value
Internet Service Type:	Bridged Service
Include Internet VLAN in Profile:	True
iMG/RG Internet VC/VLAN Id (2..4094):	20
Use PPPoE:	
iMG/RG Local Customer VLAN Id (2..4094):	
Use DHCP to obtain WAN IP Address:	False
DNS Servers (list of IP Addrs. or None):	
Local IP Address:	
Local Mask:	
Local DHCP Start IP Address:	
Local DHCP End IP Address:	
Rate Limiting:	Disabled
Up. Rate Limit (1..50000 kbps):	
Up. Burst Size (1..67108 bps):	
Up. Scalar (1..100):	
Down. Rate Limit (1..50000 kbps):	
Down. Burst Size (1..67108 bps):	
Down. Scalar (1..100):	

Copy values from profile: Routed_all_security

FIGURE 20-10 Internet Routed NAT Service - Profile "Routed/all security" - General Tab



Profile Name:

Profile Type: RG Internet

Attribute New Value

Security: Enabled

Include Security Info as part of Profile: True

Trigger Name	Type	Start Port	End Port	Max. Act. Interval
t1	tcp	10	20	30

Name	IP Address	End Address/Mask	Transport	Port	Idle	Status
m1	10.10.10.10	10.10.10.12	6	7	8	Disabled

Copy values from profile: Routed/all security

Attribute New Value

Trigger Name: t1

Secondary Start Port (1024..65535): 1024

Secondary End Port (1024..65535): 65535

Allow Multiple Hosts: Disabled

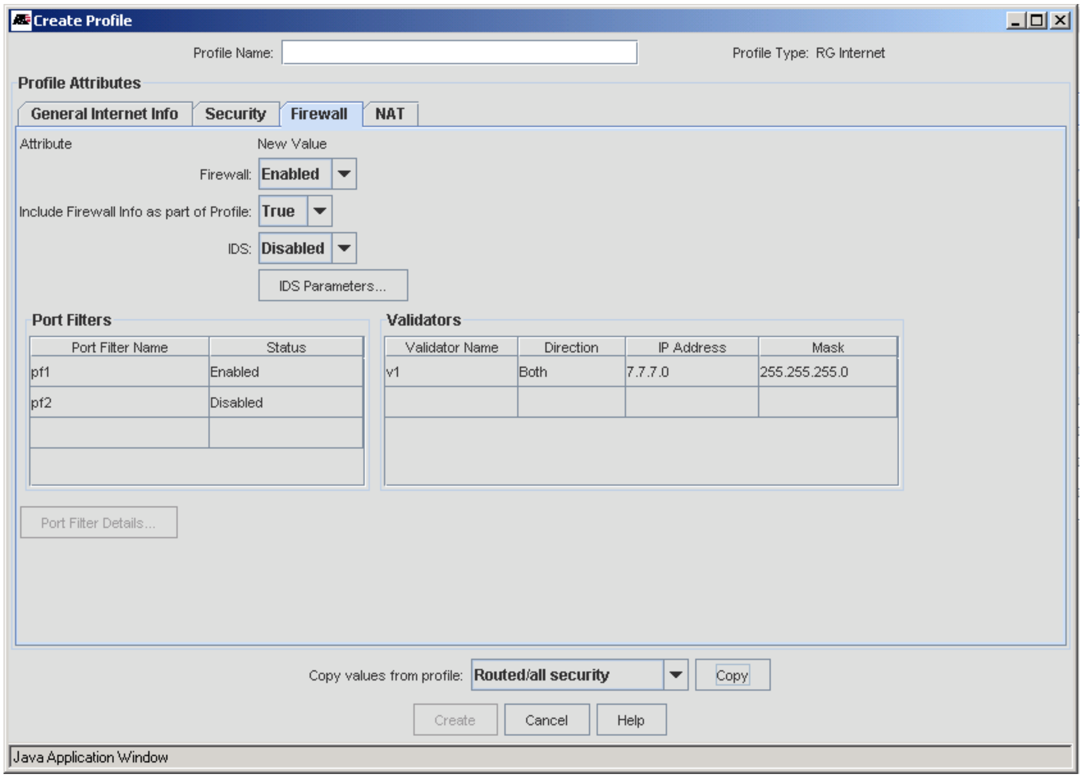
Session Chaining: Disabled

UDP Session Chaining: Disabled

Binary Address Replacement: Disabled

Address Translation Type: none

FIGURE 20-11 Internet Routed NAT Service - Profile “Routed/all security” - Security Tab



Profile Name:

Profile Type: RG Internet

Attribute New Value

Firewall: Enabled

Include Firewall Info as part of Profile: True

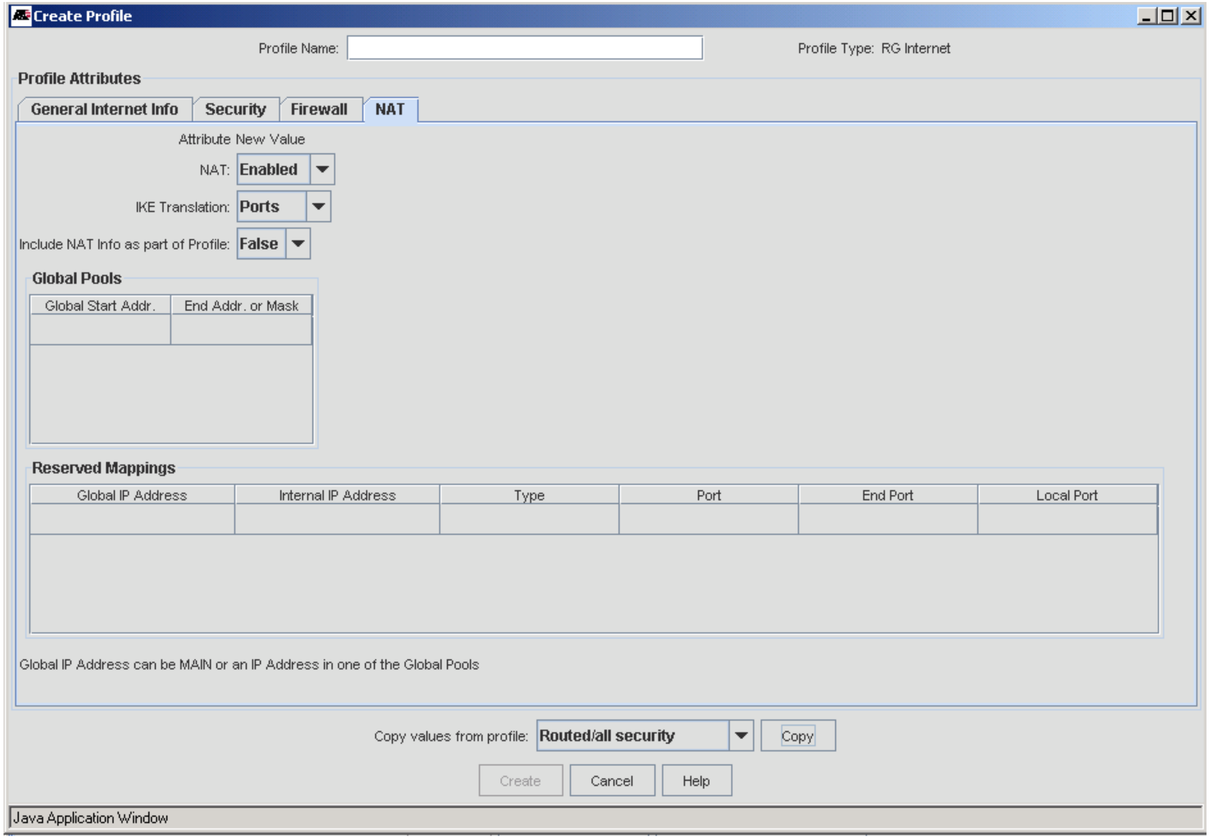
IDS: Disabled

Port Filter Name	Status
pf1	Enabled
pf2	Disabled

Validator Name	Direction	IP Address	Mask
v1	Both	7.7.7.0	255.255.255.0

Copy values from profile: Routed/all security

FIGURE 20-12 Internet Routed NAT Service - Profile “Routed/all security” - Security Tab



Profile Name:

Profile Type: RG Internet

NAT: Enabled

IKE Translation: Ports

Include NAT Info as part of Profile: False

Global Start Addr.	End Addr. or Mask

Global IP Address	Internal IP Address	Type	Port	End Port	Local Port

Global IP Address can be MAIN or an IP Address in one of the Global Pools

Copy values from profile: Routed/all security

FIGURE 20-13 Internet Routed NAT Service - Profile “Routed/all security” - NAT Tab

20.5 Video - Snooping

In Video - Snooping service, the iMAP uses the STB/MAC locking feature, so the iMAP tracks the STB usage. IGMP is enabled in the iMAP so that it can track the joins/leaves via snooping.

Refer to Figure 20-10. Note that when video is set to NONE, all video streams go to all ports, so a 100 meg data stream must be used. With snooping, the STB only gets the video stream it is requesting, which helps prevent blocking. This is especially true when there are more than two STBs.

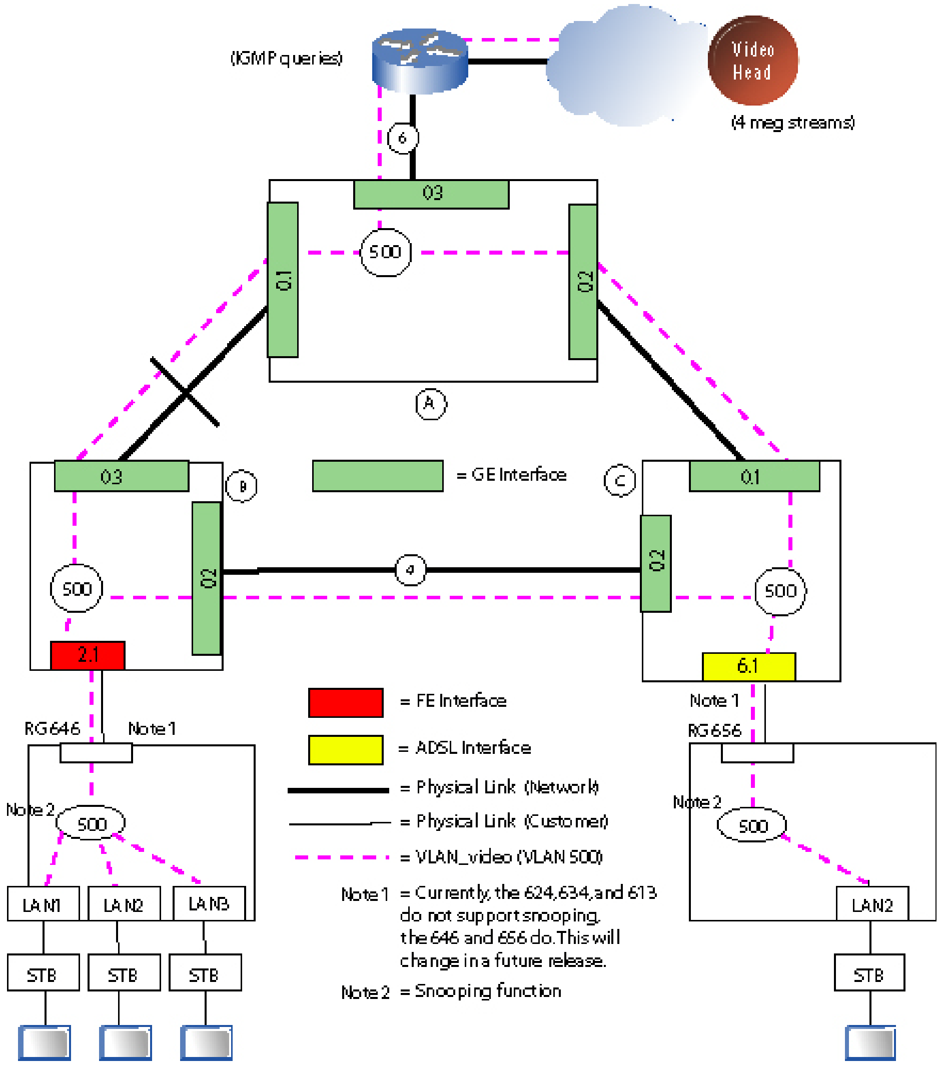
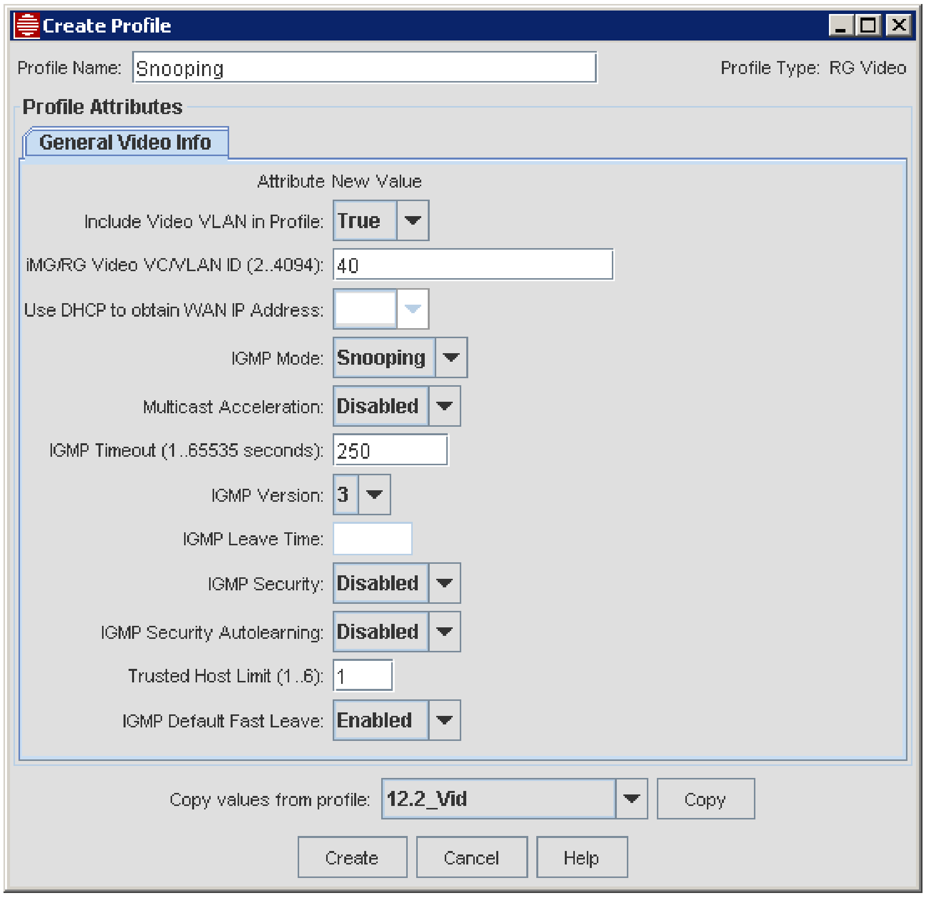


FIGURE 20-14 Video - Snooping Configuration

The following table lists the sample profiles included with the NMS and what they contain.

TABLE 20-6 Example Profiles for Video - Snooping

Profile Type	Example Profile Name	Description
RG General Profile	“Video_only”	In Mgmt. Info tab, Video VLAN (500) filled in. Port Assignment tab has one or more ports filled, as Video IP Routes not used
RG Video	“Snooping”	IGMP Node is Snooping The IGMP time-out must be at least 10 seconds greater than the router queries, but not so much higher that it will time-out. IGMP Security, Autolearning, and Trusted Host Limit are currently valid for ADSL versions of RG only. Trusted Host Limit matches number of video ports used



Profile Name: Snooping

Profile Type: RG Video

Attribute	New Value
Include Video VLAN in Profile:	True
iMG/RG Video VC/VLAN ID (2..4094):	40
Use DHCP to obtain WAN IP Address:	
IGMP Mode:	Snooping
Multicast Acceleration:	Disabled
IGMP Timeout (1..65535 seconds):	250
IGMP Version:	3
IGMP Leave Time:	
IGMP Security:	Disabled
IGMP Security Autolearning:	Disabled
Trusted Host Limit (1..6):	1
IGMP Default Fast Leave:	Enabled

Copy values from profile: 12.2_Vid

FIGURE 20-15 Video Snooping Service - Profile “Snooping”

20.6 Video - Proxy

In Video - Proxy service, the joins/leaves are performed by the RG and so IGMP is disabled on the iMAP. The iMAP supports eight Multicast groups per MAC (up to six). With proxy, the iMAP sees only one MAC, that of the RG, and up to eight MC groups. Refer to Figure 20-16.

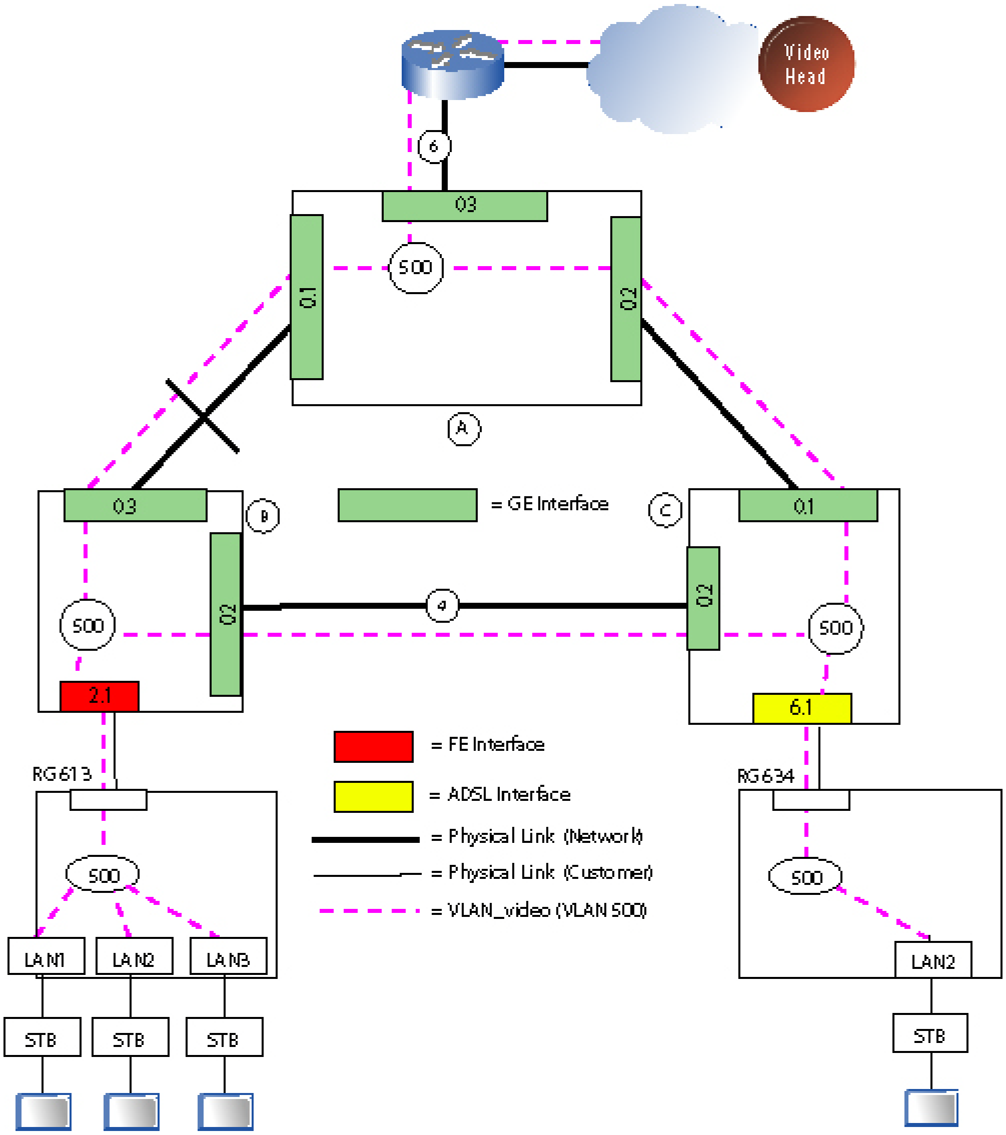
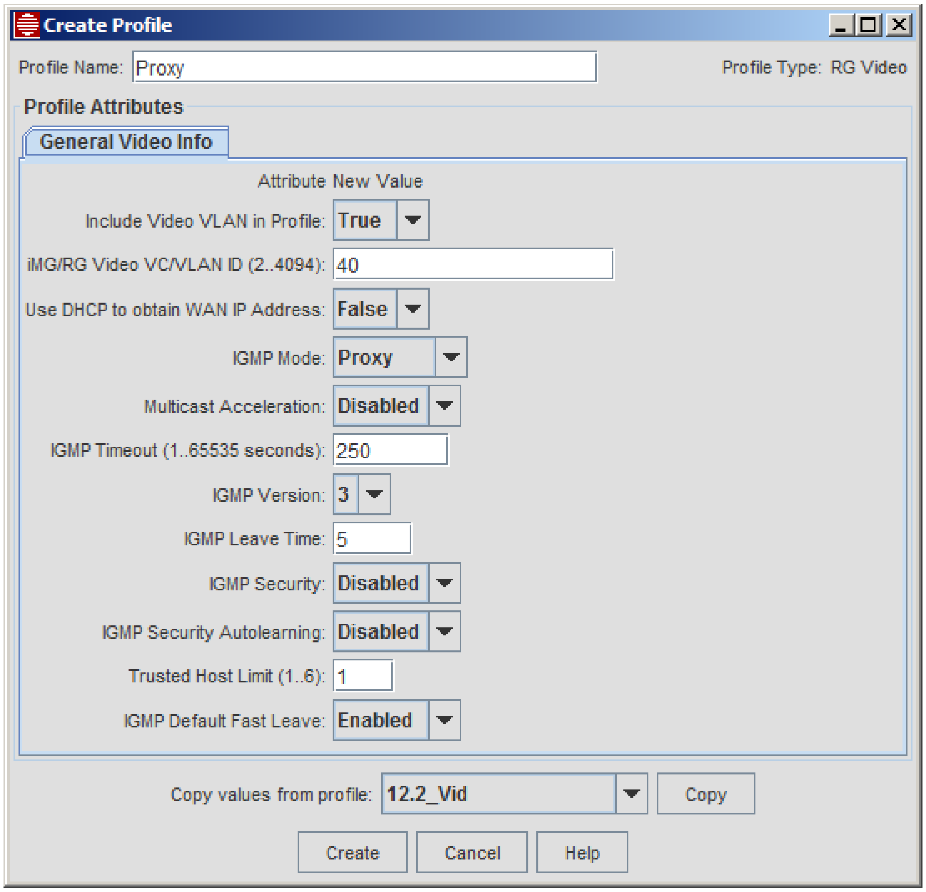


FIGURE 20-16 Video - Proxy Configuration

The following table lists the sample profiles included with the AlliedView NMS and what they contain.

TABLE 20-7 Example Profiles for Video - Proxy

Profile Type	Example Profile Name	Description
RG General Profile	"Video_only"	In Mgmt. Info tab, Video VLAN (500) filled in. Port Assignment tab has one or more ports filled, as Video IP Routes tab has no entries.
RG Video	"Proxy" (These are for ADSL only) • ManualSec2/Proxy • ManualSec3/Proxy • AutoSec2/Proxy • AutoSec3/Proxy	IGMP Node is Proxy For the others, trusted Host Limit should match number of video ports used



Profile Name: Proxy

Profile Type: RG Video

Attribute	New Value
Include Video VLAN in Profile:	True
iMG/RG Video VC/VLAN ID (2..4094):	40
Use DHCP to obtain WAN IP Address:	False
IGMP Mode:	Proxy
Multicast Acceleration:	Disabled
IGMP Timeout (1..65535 seconds):	250
IGMP Version:	3
IGMP Leave Time:	5
IGMP Security:	Disabled
IGMP Security Autolearning:	Disabled
Trusted Host Limit (1..6):	1
IGMP Default Fast Leave:	Enabled

Copy values from profile: 12.2_Vid

FIGURE 20-17 Video Proxy Service - Profile "Proxy"

20.7 Voice - Public and Private

For voice service, a major choice is whether to include voice service on an internet VLAN (Public) or to use a separate VLAN for voice (Private). This choice, as well as whether IP addresses will be allocated statically or dynamically, are attributes for each type of Voice service. Moreover, each of these services is on an RG basis; the specific service types cannot be shared on the same RG. (In most cases, an ISP has one main strategy for providing voice service and so applies the same service to all RGs.) Refer to Figure 20-18.

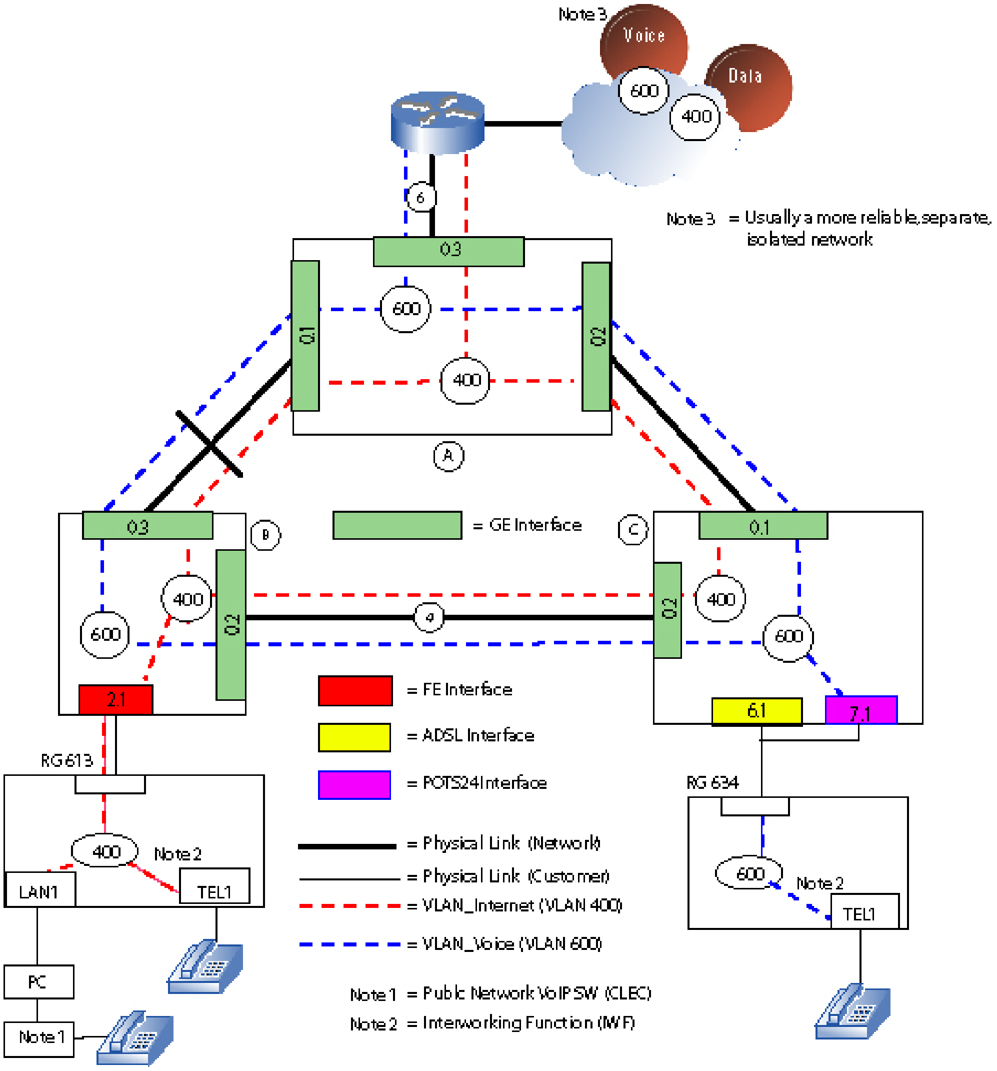
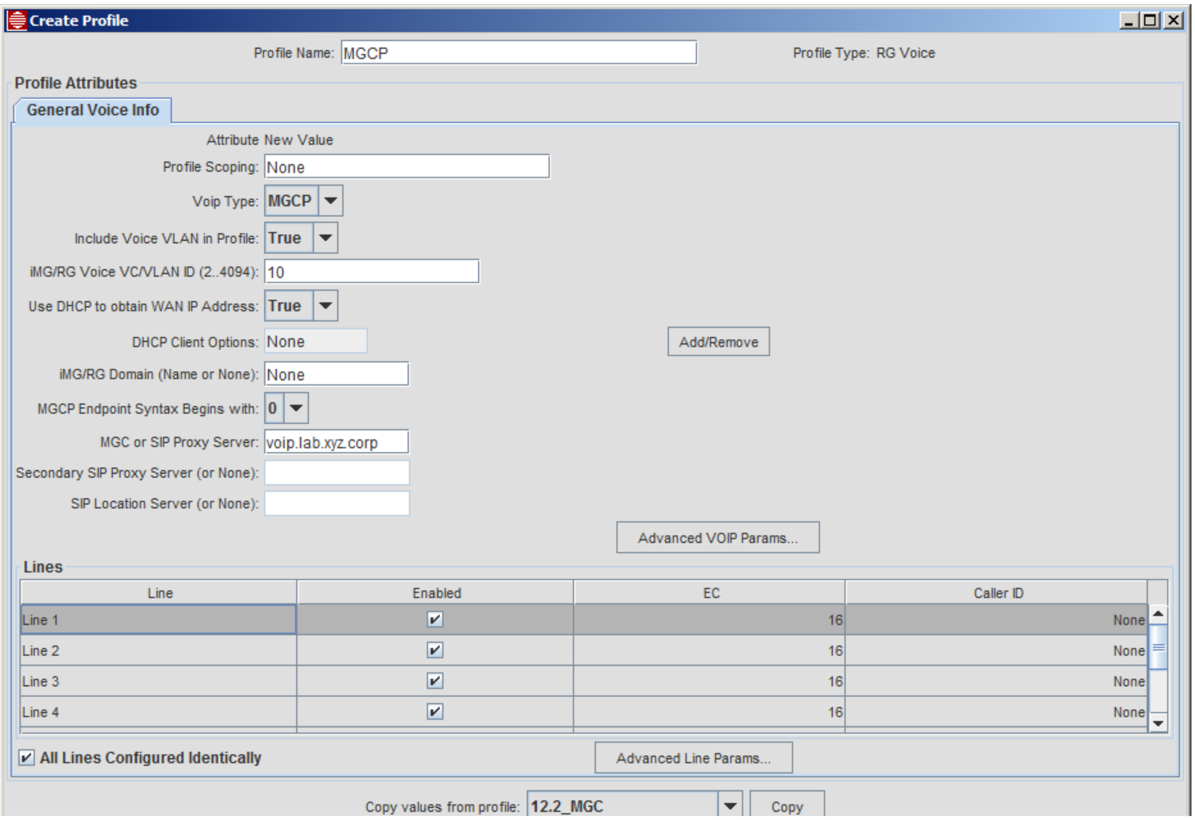

Note 3
Voice
Data
600
400
6
03
600
400
01
02
A
= GE Interface
B
C
03
02
400
600
4
01
02
400
600
2.1
6.1
7.1
= FE Interface
= ADSL Interface
= POTS24 Interface
RG613
RG 634
400
Note 2
LAN1
TEL1
PC
Note 1
600
Note 2
TEL1
= Physical Link (Network)
= Physical Link (Customer)
= VLAN_Internet (VLAN 400)
= VLAN_Voice (VLAN 600)
Note 3 = Usually a more reliable, separate, isolated network
Note 1 = Public Network VoIP SW (CLEC)
Note 2 = Interworking Function (IWF)

FIGURE 20-18 Voice - Public and Private Configuration

The following table lists the sample profiles included with the AlliedView NMS and what they contain.

TABLE 20-8 Example Profiles for Voice

Profile Type	Example Profile Name	Description
RG General Profile	“Voice_only”	In Mgmt. Info tab, Voice VLAN (600) filled in. Port Assignment tab has no ports datafilled. IP Routes tab has Route 1 enabled, and then subnet and subnet mask of Media Gateway Controller, and Gateway address that connects to the Media Gateway Controller
RG Voice	“RG-POTS-4Line”	Profile Scoping is None VOIP Type is MGCP GBG6 Service path is Private Path, since a separate Voice VLAN iMG/RG Domain used in voip subnet configuration. Refer to Dynamic DNS Naming for Voice Subnets.
	“SIP1”	This provides most of the attributes for the SIP configuration. Note that there is the “Advanced Line Params” where additional parameters are entered. This button is activated when at least one of the lines is Enabled.



Create Profile

Profile Name: MGCP

Profile Type: RG Voice

Profile Attributes

General Voice Info

Attribute	New Value
Profile Scoping:	None
Voip Type:	MGCP
Include Voice VLAN in Profile:	True
iMG/RG Voice VC/VLAN ID (2..4094):	10
Use DHCP to obtain WAN IP Address:	True
DHCP Client Options:	None
iMG/RG Domain (Name or None):	None
MGCP Endpoint Syntax Begins with:	0
MGC or SIP Proxy Server:	voip.lab.xyz.corp
Secondary SIP Proxy Server (or None):	
SIP Location Server (or None):	

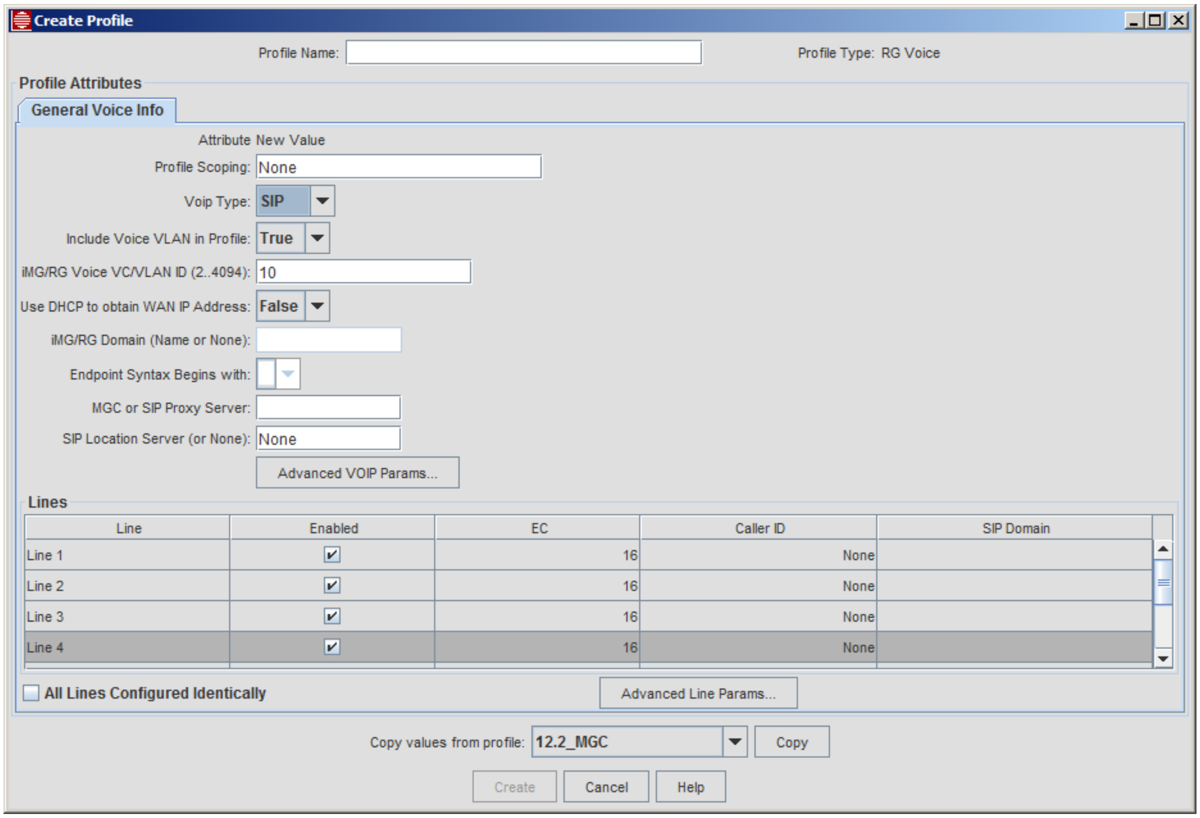
Lines

Line	Enabled	EC	Caller ID
Line 1	☑	16	None
Line 2	☑	16	None
Line 3	☑	16	None
Line 4	☑	16	None

☑ All Lines Configured Identically

Copy values from profile: 12.2_MGC

FIGURE 20-19 Voice Service - Profile “RG-POTS-4Line”



Profile Name:

Profile Type: RG Voice

Profile Attributes

Attribute	New Value
Profile Scoping:	None
Voip Type:	SIP
Include Voice VLAN in Profile:	True
iMG/RG Voice VC/VLAN ID (2..4094):	10
Use DHCP to obtain WAN IP Address:	False
iMG/RG Domain (Name or None):	
Endpoint Syntax Begins with:	
MGC or SIP Proxy Server:	
SIP Location Server (or None):	None

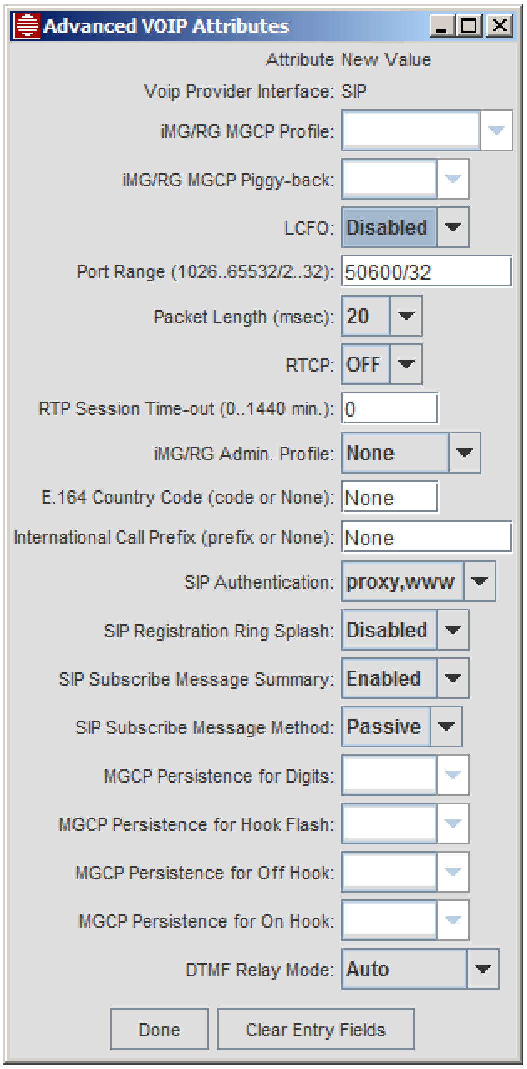
Lines

Line	Enabled	EC	Caller ID	SIP Domain
Line 1	☑	16	None	
Line 2	☑	16	None	
Line 3	☑	16	None	
Line 4	☑	16	None	

□ All Lines Configured Identically

Copy values from profile: 12.2_MGC

FIGURE 20-20 RG Voice Profile - “SIP1”



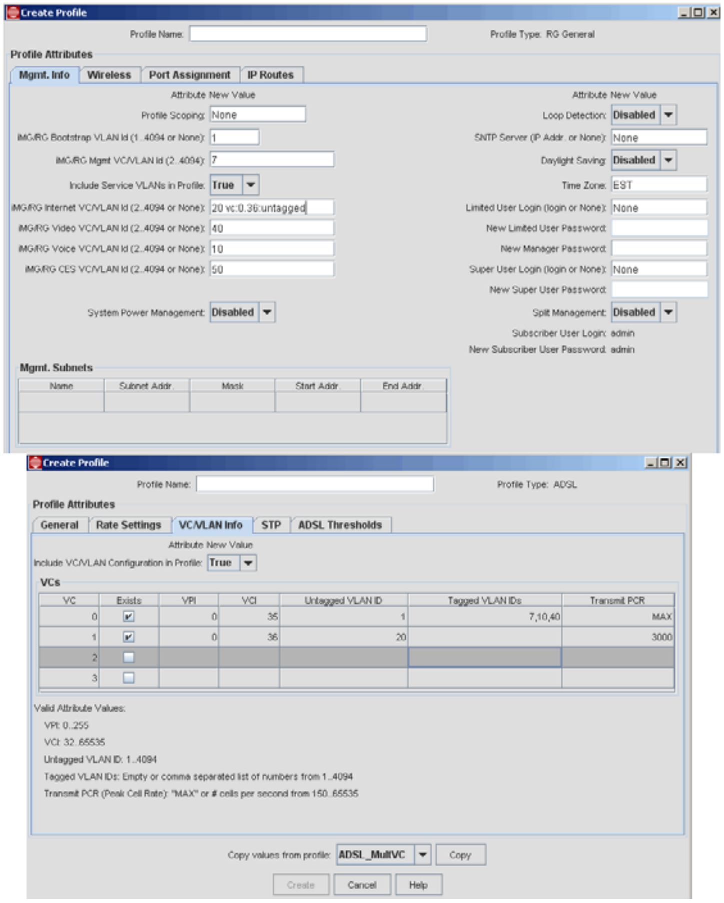
Advanced VOIP Attributes

Attribute	New Value
Voip Provider Interface:	SIP
iMG/RG MGCP Profile:	
iMG/RG MGCP Piggy-back:	
LCFO:	Disabled
Port Range (1026..65532/2..32):	50600/32
Packet Length (msec):	20
RTCP:	OFF
RTP Session Time-out (0..1440 min.):	0
iMG/RG Admin. Profile:	None
E.164 Country Code (code or None):	None
International Call Prefix (prefix or None):	None
SIP Authentication:	proxy,www
SIP Registration Ring Splash:	Disabled
SIP Subscribe Message Summary:	Enabled
SIP Subscribe Message Method:	Passive
MGCP Persistence for Digits:	
MGCP Persistence for Hook Flash:	
MGCP Persistence for Off Hook:	
MGCP Persistence for On Hook:	
DTMF Relay Mode:	Auto

FIGURE 20-21 RG Voice Profile for "SIP1" - Advanced VOIP Attributes

20.8 ADSL iMG with multiple VCs

The user can provision the iMG/RG General Profile and ADSL Port Profile so that the ADSL-based iMG/RG can support service VLANs with different VC configurations. The format used to specify a specific VLAN/VC combination is <vlanid> vc:<vpi>.<vci>:<tagged or untagged>. In the following figure, the RG General Profile has the internet VLAN configured on a different VC with VPI=0 and VCI=36. An ADSL port profile is then created to match that setting, as well as the transmit rates.



Profile Name:
Profile Type: RG General

Attribute New Value

Profile Scoping: None
iMG/RG Bootstrap VLAN Id (1..4094 or None): 1
iMG/RG Mgmt VC/VLAN Id (2..4094): 7
Include Service VLANs in Profile: True
iMG/RG Internet VC/VLAN Id (2..4094 or None): 20 vc:0.36:untagged
iMG/RG Video VC/VLAN Id (2..4094 or None): 40
iMG/RG Voice VC/VLAN Id (2..4094 or None): 10
iMG/RG CES VC/VLAN Id (2..4094 or None): 50
System Power Management: Disabled

Attribute New Value

Loop Detection: Disabled
SNTP Server (IP Addr. or None): None
Daylight Saving: Disabled
Time Zone: EST
Limited User Login (login or None): None
New Limited User Password:
New Manager Password:
Super User Login (login or None): None
New Super User Password:
Split Management: Disabled
Subscriber User Login: admin
New Subscriber User Password: admin

Name	Subnet Addr.	Mask	Start Addr.	End Addr.

Profile Name:
Profile Type: ADSL

Attribute New Value

Include VC/VLAN Configuration in Profile: True

VC	Exists	VPI	VCI	Untagged VLAN ID	Tagged VLAN IDs	Transmit PCR
0	☑	0	35	1	7,10,40	MAX
1	☑	0	36	20		3000
2	□					
3	□					

Valid Attribute Values:

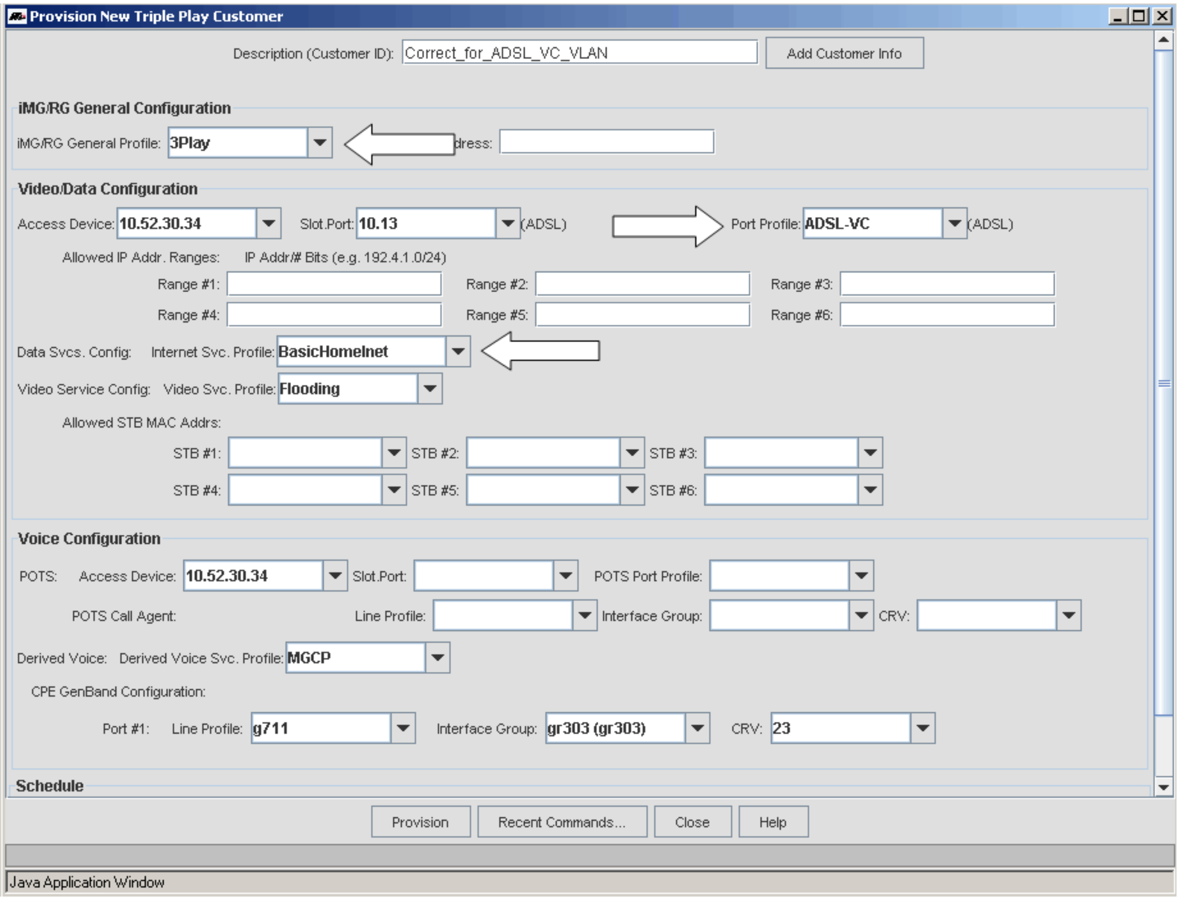
VPI: 0..255
VCI: 32..65535
Untagged VLAN ID: 1..4094
Tagged VLAN IDs: Empty or comma separated list of numbers from 1..4094
Transmit PCR (Peak Cell Rate): "MAX" or # cells per second from 150..65535

Copy values from profile: ADSL_MultVC

FIGURE 20-22 The RG General and ADSL Port Profile to Support VLAN/VC Configuration

When the user then fills out the Triple-Play form for the ADSL-based iMG/RG, and uses these profiles, the VLAN/VC settings will be set immediately on the iMAP, and on the iMG/RG when it placed into service (connected and powered on). The following figure shows a Triple-Play form that uses the profiles that will have the iMG/RG come up with the internet VLAN having a different VC and transmit rate, as shown in Figure 20-22.

Note: *The attributes on the iMG/RG General Profile, Port Profile, and Service Profile must match. Otherwise, when the user fills out and submits the Triple Play form, it will fail with the error message that the profiles don't match. (If these profiles were to be applied, traffic would not pass on the internet VLAN.) This is shown next.*



Description (Customer ID): Correct_for_ADSL_VC_VLAN

iMG/RG General Profile: 3Play

Access Device: 10.52.30.34 Slot.Port: 10.13 (ADSL) Port Profile: ADSL-VC (ADSL)

Data Svcs. Config: Internet Svc. Profile: BasicHomeInet

Video Service Config: Video Svc. Profile: Flooding

POTS: Access Device: 10.52.30.34

Derived Voice: Derived Voice Svc. Profile: MGCP

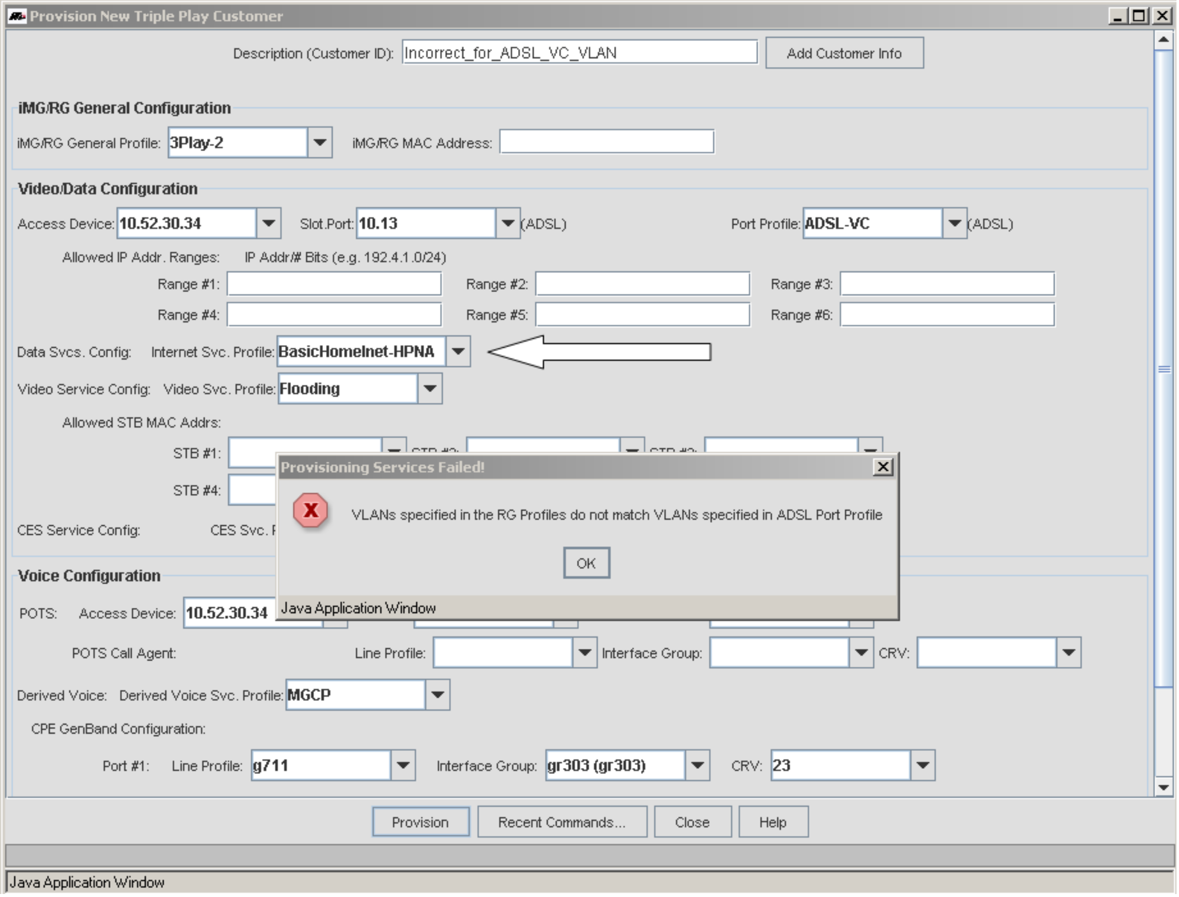
CPE GenBand Configuration:

Port #1: Line Profile: g711 Interface Group: gr303 (gr303) CRV: 23

FIGURE 20-23 Triple Play Form with Profiles to Configure VLAN/VC for Internet Service

The user also must be aware that when provisioning an ADSL iMG/RG, the profiles must be aligned so that the services can be provisioned. The main guidelines are:

- When specifying the VC in an iMG/RG profile, and the profile is applied to a non-DSL iMG/RG, the VPI, VCI, and Framing attributes are ignored.
- If the user fills out the Triple-Play form and uses profiles that do not match up with each other for VLAN/service configuration, the NMS will not allow the subscriber to be provisioned and will display an error message. Refer to the following figure.



Description (Customer ID): Incorrect_for_ADSL_VC_VLAN

iMG/RG General Configuration

iMG/RG General Profile: 3Play-2 iMG/RG MAC Address:

Video/Data Configuration

Access Device: 10.52.30.34 Slot.Port: 10.13 (ADSL) Port Profile: ADSL-VC (ADSL)

Allowed IP Addr. Ranges: IP Addr/# Bits (e.g. 192.4.1.0/24)

Range #1: Range #2: Range #3:

Range #4: Range #5: Range #6:

Data Svcs. Config: Internet Svc. Profile: BasicHomeInet-HPNA

Video Service Config: Video Svc. Profile: Flooding

Allowed STB MAC Addrs:

STB #1:

STB #4:

CES Service Config: CES Svc. P

Provisioning Services Failed!

VLANs specified in the RG Profiles do not match VLANs specified in ADSL Port Profile

Voice Configuration

POTS: Access Device: 10.52.30.34

POTS Call Agent: Line Profile: Interface Group: CRV:

Derived Voice: Derived Voice Svc. Profile: MGCP

CPE GenBand Configuration:

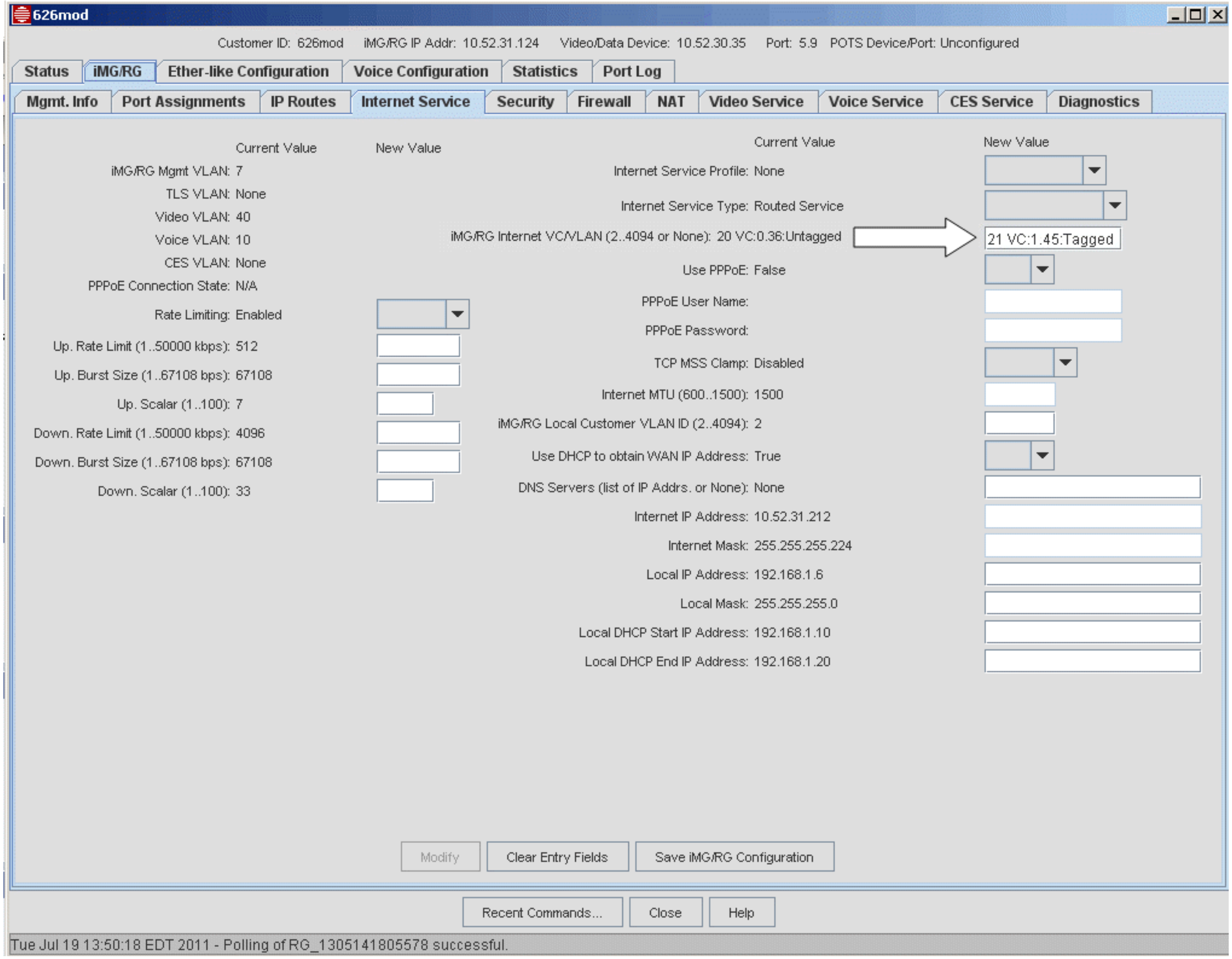
Port #1: Line Profile: g711 Interface Group: gr303 (gr303) CRV: 23

FIGURE 20-24 Provisioning Error for DSL-based iMG/RG

Once the iMG/RG is provisioned and in service, the user has the option to change the settings in the Triple Play Service Management window. Moreover, once this is updated, the NMS will update the iMAP port configuration if necessary.

In the following figure, the user has decided to change the internet VLAN so that it is on VLAN 21 (rather than 20), and has VPI=1, VCI=45. The user can go to the Service Management window and in the *iMG/RG->Internet Service* tab change the iMG/RG Internet VC/VLAN to 21 VC:1.45:Tagged. Refer to the following figure.

Note: *The user should avoid making changes on the Service Management Form when possible, since if the value entered here is different than what is in the iMG/RG General or Service Profile, the device will be marked as out-of-sync.*



Customer ID: 626mod iMG/RG IP Addr: 10.52.31.124 Video/Data Device: 10.52.30.35 Port: 5.9 POTS Device/Port: Unconfigured

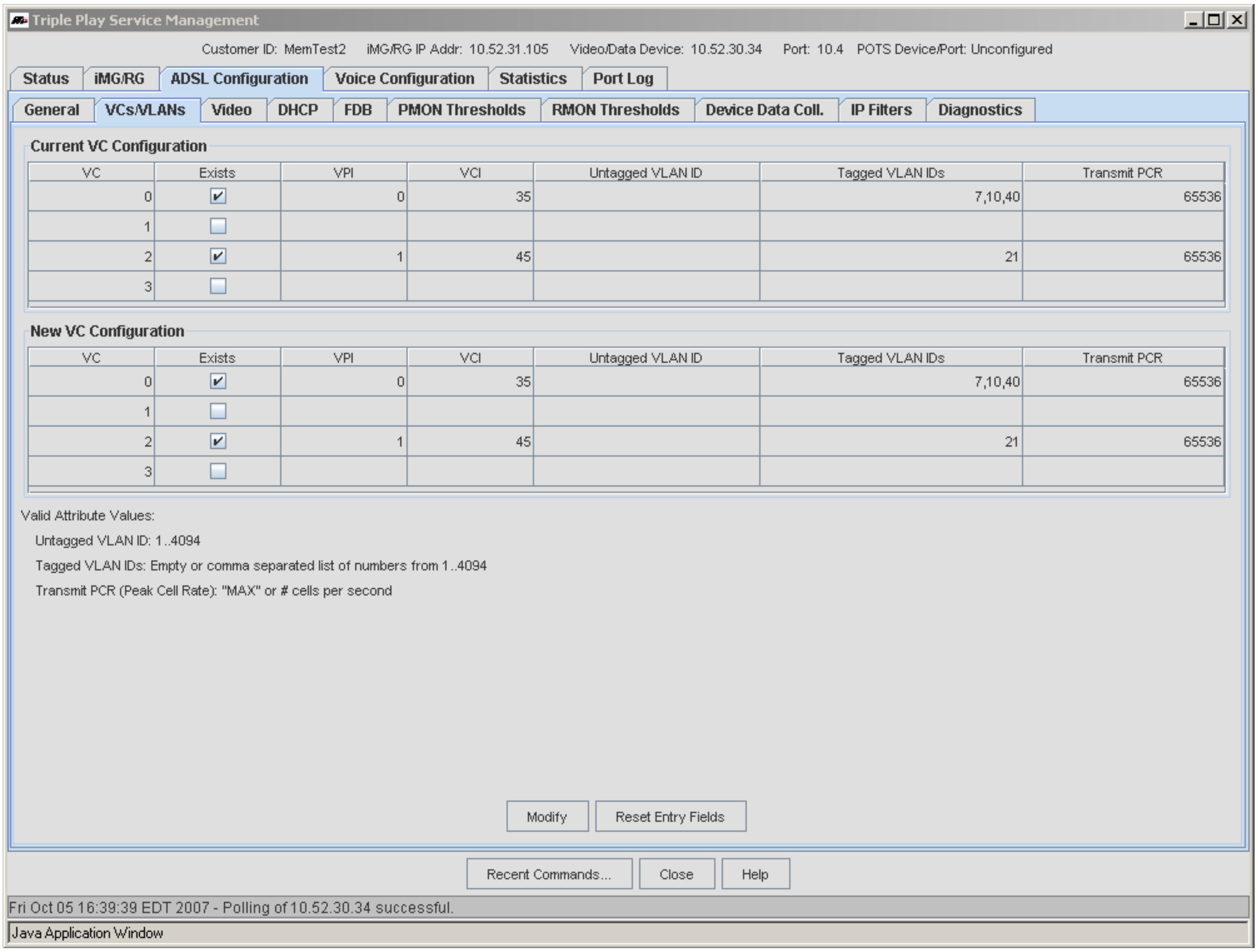
	Current Value	New Value
iMG/RG Mgmt VLAN:	7	
TLS VLAN:	None	
Video VLAN:	40	
Voice VLAN:	10	
CES VLAN:	None	
PPPoE Connection State:	N/A	
Rate Limiting:	Enabled	
Up. Rate Limit (1..50000 kbps):	512	
Up. Burst Size (1..67108 bps):	67108	
Up. Scalar (1..100):	7	
Down. Rate Limit (1..50000 kbps):	4096	
Down. Burst Size (1..67108 bps):	67108	
Down. Scalar (1..100):	33	

	Current Value	New Value
Internet Service Profile:	None	
Internet Service Type:	Routed Service	
iMG/RG Internet VC/VLAN (2..4094 or None):	20 VC:0.36:Untagged	21 VC:1.45:Tagged
Use PPPoE:	False	
PPPoE User Name:		
PPPoE Password:		
TCP MSS Clamp:	Disabled	
Internet MTU (600..1500):	1500	
iMG/RG Local Customer VLAN ID (2..4094):	2	
Use DHCP to obtain WAN IP Address:	True	
DNS Servers (list of IP Addrs. or None):	None	
Internet IP Address:	10.52.31.212	
Internet Mask:	255.255.255.224	
Local IP Address:	192.168.1.6	
Local Mask:	255.255.255.0	
Local DHCP Start IP Address:	192.168.1.10	
Local DHCP End IP Address:	192.168.1.20	

Tue Jul 19 13:50:18 EDT 2011 - Polling of RG_1305141805578 successful.

FIGURE 20-25 Changing an existing VLAN/VC Configuration

After choosing Save iMG/RG Configuration, the user will see that the NMS will make the necessary changes, and in the *ADSL Configuration -> VCs/VLANs* tab the changes are reflected. Refer to the following figure.



Customer ID: MemTest2 iMG/RG IP Addr: 10.52.31.105 Video/Data Device: 10.52.30.34 Port: 10.4 POTS Device/Port: Unconfigured

Current VC Configuration

VC	Exists	VPI	VCI	Untagged VLAN ID	Tagged VLAN IDs	Transmit PCR
0	☑	0	35		7,10,40	65536
1	□					
2	☑	1	45		21	65536
3	□					

New VC Configuration

VC	Exists	VPI	VCI	Untagged VLAN ID	Tagged VLAN IDs	Transmit PCR
0	☑	0	35		7,10,40	65536
1	□					
2	☑	1	45		21	65536
3	□					

Valid Attribute Values:

Untagged VLAN ID: 1..4094

Tagged VLAN IDs: Empty or comma separated list of numbers from 1..4094

Transmit PCR (Peak Cell Rate): "MAX" or # cells per second

Fri Oct 05 16:39:39 EDT 2007 - Polling of 10.52.30.34 successful.

FIGURE 20-26 Result of changing VLAN/VC for Internet Service

Note: If all four VCs are being used and the user wishes to change a VPI/VCI attributes for one of the existing VCs, this cannot be done; the user must delete one of the VCs and then add the new VPI/VCI combination to a new VC.

21. Provisioning iMGs

Allied Telesis Residential Gateway (RG) and intelligent Multiservice Gateway (iMG) products provide advanced IP Triple Play voice, video and data services to subscribers.

Note: *The terms "RG" and "iMG" are used interchangeably in both the NMS client user interface and in this document. Unless explicitly stated, anything that applies to an iMG applies to an RG, and vice versa.*

Provisioning involves:

- **DHCP Discovery**: DHCP discovery ensures that an iMG is configured with the correct software and IP address as part of the DHCP messaging that takes place between the iMG, DHCP server, and the NMS with its TFTP server.
- **Profiles**: Profiles provide a set of templates you can apply to one or more iMGs to ensure they are provisioned with the correct attributes for a specific service type. There are two main types of profiles:
  - General: General profiles are associated with iMGs regardless of the types of services the iMG provides.
  - Service: Service profiles contain attributes that are service-specific. They are associated with a device to configure a specific service.
- **Triple-Play**: The Triple-Play form streamlines upstream port provisioning and includes iMG attributes. The fields that appear and are data filled are driven by the profiles that are included with the form.

21.1 Naming Conventions to Identify Components (DNS)

The DNS naming conventions for components are extremely important for administrators because they help in allowing services to be delivered to subscribers within a specific Access Island.

Note: *When dynamic DNS services are required (as in the case of the G6) the voice DHCP server must be separate from the rgboot/rgmgmt. The DNS servers can be on separate servers or they can coexist on DHCP servers.*

For the iMAPs, the remoteID is used as part of the DNS name, and it follows a very specific naming convention, as explained in DNS Entries for Allied Telesis Components (iMAPs). The DNS server will scope on the first set of digits (depending on the naming convention used) of the remote-ID, which identifies a specific Access Island. This, along with the VLAN IDs and Vendor-Class ID, determine which layer 3 subnets should be used for a specific subscriber. This is explained in detail in DNS Entries for Allied Telesis Components (iMAPs).

For all of the iMG/RGs within a specific voice subnet, there must be a DNS entry with a structured name. When configured correctly (for the DNS servers and the AlliedView NMS Profiles) the AlliedView NMS correctly coordinates the voice components so that voice service works correctly. This is explained in detail in Dynamic DNS Naming for Voice Subnets.

Note: *Before beginning the configuration of iMGs/RGs, the naming system should be planned out, and then set up in the DNS or a local host file.*

Note: *You must add RGMgmt subnets to discovered and managed subnets before any devices can be discovered on these subnets.*

21.1.1 DNS Entries for Allied Telesis Components (iMAPs)

The naming of the iMAPs identifies the Service Area (the Access Island) and how it maps to service locations. Each iMAP component includes an identification ID (remoteID in the DHCP instance) that includes this Service Area, Service Location, and Access Island number. It then includes the specific iMAP. Table 21-1 explains this naming, with the result as follows:

- The Service Area is SPSI
- The specific Access Island the component is part of is included as well (AI1 for Access Island 1)

All components use this prefix as part of their ID and are used for DNS naming.

TABLE 21-1 Recommended Naming Convention for Remote ID of iMAP for DHCP

Attribute	Value
CCCCSS-AInn-LLnTTnn	General format for Remote ID (See below)
CCCC	4 character name for the serving area
SS-	2 character name for the state the serving area is located in.A dash at the end helps to identify the Access Island, which is next in the string. This is optional.
AInn-	The Access Island that this device belongs in, so AI01 1 would be Access Island 1. For a test Access Island, a 00 or T instead of a number would be used. Note there is a dash (-) after the Access Island. This allows the user to more easily discern the digits that identify the Access Island These make up the10-digit prefix that identifies the Access Island. Also, this is used to scope Profiles.
nnnn....	Characters that help identify the device and any attributes for its location, type, etc.
Examples	iMAP 1 9700 = SPSI-AI00-MAP1x7 iMAP 2 9400 = SPSI-AI00-MAP2x4 iMAP 5 9810 = SPSI-AI00-MAP5x8 x3112 NCSU = SPSI-AI00-x3112-NCSU

With the domain suffix of “ai.corp.int”:

The fully qualified name for the first iMAP would be:

SPSI-AI00-MAP1x7.ai.corp.int

The following table summarizes the naming convention.

TABLE 21-2 Reference for Remote ID

Description	4 character name for the serving area	2 character name for the state the serving area is located in.	Access Island that this device belongs in, separated by a dash. Use one dash on each side to help in reading the string. this part of the string. Do not use double dashes or spaces in the string.	Characters used to identify the device and any attributes that are significant.
Example Values	SPSI	NA	-AI00- -AI01- -AIT- (test)	MAP1x7

21.1.2 Character Usage Rules

- Character allowed are letters, numbers, single dashes (-), and periods (.).
- Do not use a double dash, such as when you need a placeholder. Instead, use a string such as -X-.
- Do not use spaces, underscores, colons, or other special characters.

21.1.3 Dynamic DNS Naming for Voice Subnets

For voice service, there must be a Dynamic DNS entry for all RGs in the voice subnet. Moreover, each entry must have a specific structured name (Fully Qualified Domain Name, or FQDN) so that all related components can communicate with each other and be aware when changes are made. The format of the FQDN is as follows:

rgvoip-<MAC address>.domain

This is part of the DHCP discovery process, and its success depends on the components that make up voice service being configured and pre-provisioned correctly. This is explained in detail in Discovering Voice Subnets (GenBand, MGC Protocol).

21.2 Provisioning Tasks

Provisioning an iMG requires a series of tasks, including:

- Set up the DHCP configuration on the DHCP server(s) and upstream devices.
- Create profiles.
- Provision the Triple Play form for each customer using an iMG.
- Install the iMG.
- Apply power to the iMG and wait for the key indicators (lights) to indicate when the iMG is configured and running. The iMG will cycle through its initial and reboot sequence.
- Attach any customer devices to the iMG.
- Set up custom views in the NMS to view the iMG configurations.
- Update configurations as necessary.

You can perform these tasks in different orders, for example:

- **Fill in the Triple Play form before you apply power to the** iMG. With this strategy, when you apply power to the iMG, the iMG configuration and connection to the upstream device is automatically applied. This is the most common sequence for a new customer and is the strategy used in the example installation procedures, where the pre-provisioned configuration is downloaded to the iMG at the end of the DHCP and discovery process.
- **Fill in the Triple play form after you apply power to the** iMG. With this strategy, you provision an iMG as you fill out the Triple Play form for each port, then apply the configuration to the iMG. You can provision devices immediately or on a schedule.
- **Use the new configuration tasks to re-engineer a previously installed** iMG. You can use this strategy when services are changing to associate the appropriate profiles with the device, or to apply new configuration settings. You can use the iMG Boot Load Configurator for this strategy.

21.3 Configuring Components for DHCP Discovery

For an iMG to be discovered using DHCP, you must configure the following tools and files correctly:

- iMG Boot Load Configurator
- DHCP Server File (dhcpd.conf)
- DHCP Relay Configured on the iMAPs (VLAN Configuration)
- DHCP Relay Configured on the AlliedWare Plus Devices (VLAN Configuration)

Note: *For iMGs to use DHCP correctly, all iMAP and AlliedWare Plus devices must use DHCP Relay, not DHCP Snooping. Refer to the Software Reference for iMAP Series Switches and the Allied Telesis Software Reference for AlliedWare Plus Operating System for details on the differences between the two types of DHCP.*

21.4 iMG Boot Load Configurator

The iMG Boot Load Configurator creates bootstrap configurations for the SNMP and CWMP iMG types. The bootstrap configuration can include:

- firmware
- snmpinit file - defines the device's SNMP communities
- snmpd.cnf file - includes defining the device's trap host
- im.conf file - includes defining the device's management VLAN identifier
- MD5SUM file - used by iMGs as a guide to which files need to be downloaded
- cm.bsvlan[x]t file - This file is used to set up the Mgmt VLAN (the number entered in the Mgmt VLAN ID field) and DHCP using the VLAN to configure the iMG. The [x] in the file name depends on the Mgmt VLAN.

The iMG Boot Load Configurator creates bootstrap configurations for all iMG types. The bootstrap configurations serve as a uniform starting point for customer provisioning as iMGs are added to a managed network. The configurator then places the bootstrap loads into the NMS TFTP server directory tree, where they are accessible to iMGs as TFTP clients.

An iMG downloads bootstrap configuration files via TFTP when it first boots up over the default VLAN. The bootstrap configuration initializes the iMG's management VLAN, SNMP settings, and software release.

Caution: Use the iMG Boot Load Configurator with caution. The loads it creates must be consistent with the DHCP configuration, which is not integrated into the tool. The iMG Boot Load Configurator creates loads with whatever parameters are entered, so be sure the parameters are valid and meaningful. To correct mistakes, repeat the process and overwrite invalid loads.

21.4.1 Launching the iMG Boot Load Configurator

You launch the iMG Boot Load Configurator from the NMS server. To launch the tool, navigate to the /bin directory under the AlliedView NMS installation directory and run the following:

- On Windows, run **AT_BootConfigurator.bat**.
- On Linux, run **/AT_BootConfigurator.sh**.

On Windows, you can also launch the iMG Boot Load Configurator from the Start menu:

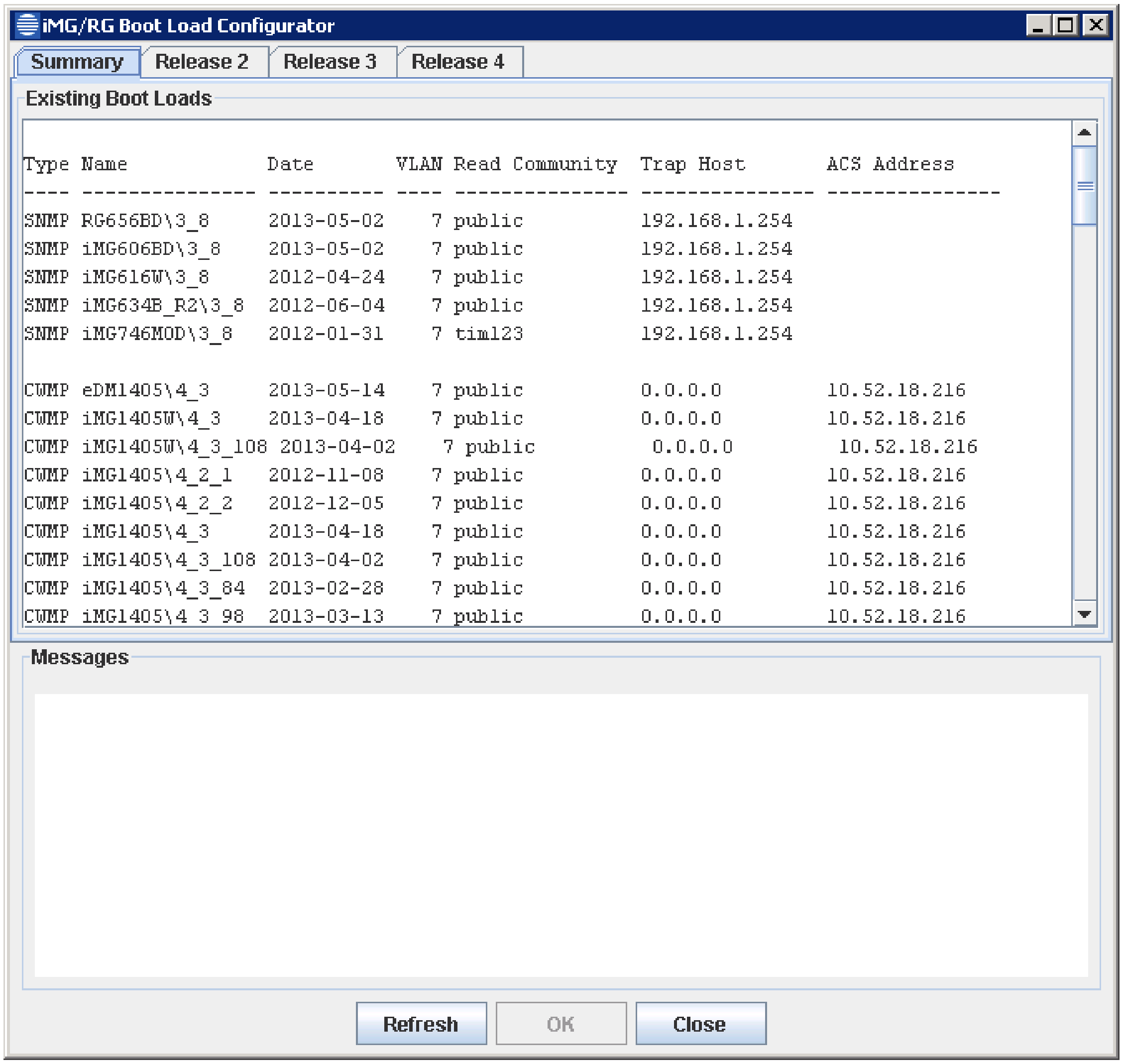
Allied Telesis > AlliedView NMS > Tools > RG Boot Configurator

The iMG Boot Load Configurator contains four tabs:

- Summary
- Release 2
- Release 3
- Release 4

21.4.2 Summary

The **Summary** tab lists the existing configurations. Release 2 snd 3 configurations are grouped as SNMP types and Release 4 configurations are grouped as CWMP types. The **Refresh** button, which is only enabled on the Summary tab, refreshes the display and adds any new configurations you create.



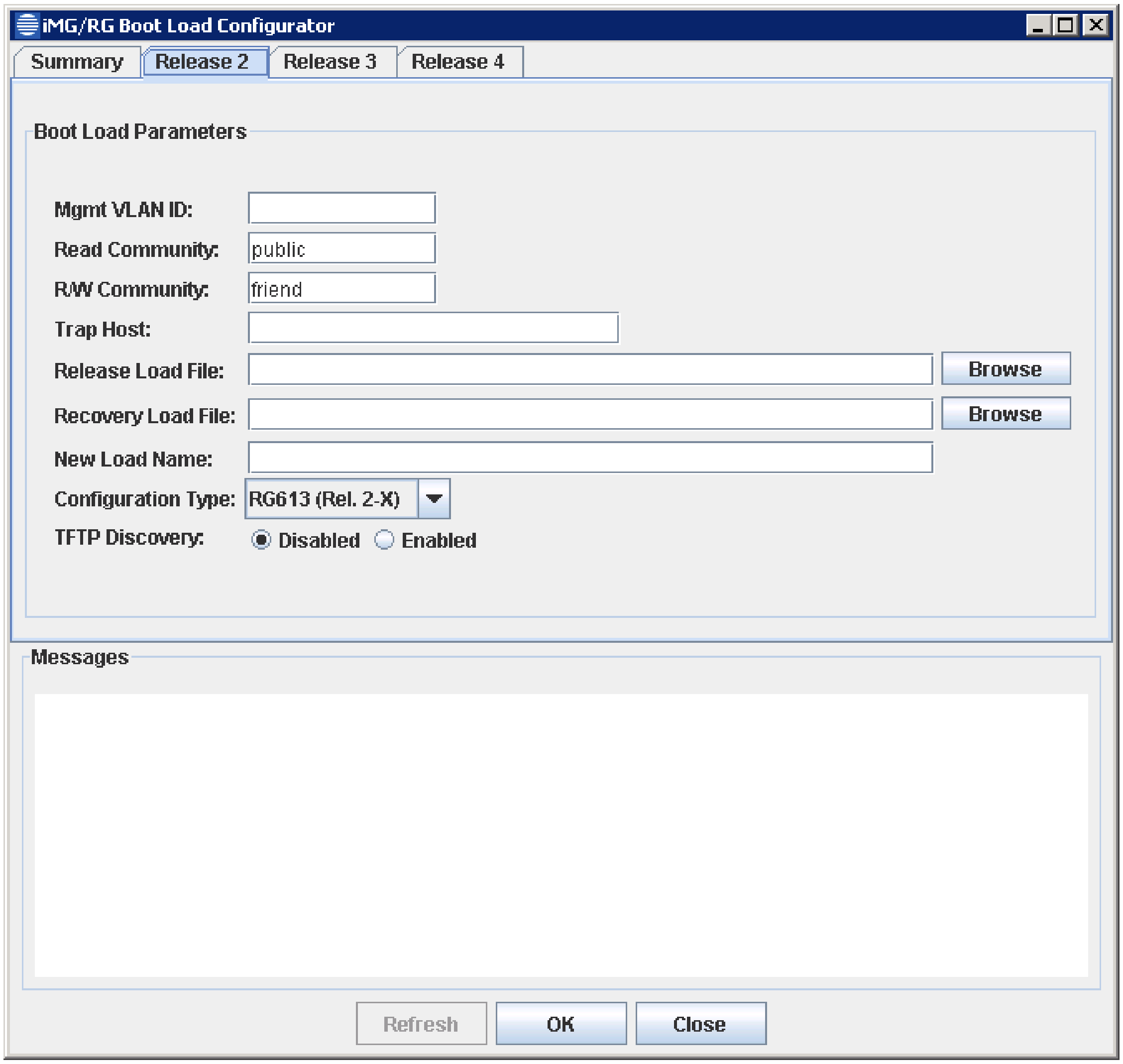
```
Type Name            Date       VLAN Read Community  Trap Host       ACS Address
---- --------------- ---------- ---- --------------- --------------- ---------------
SNMP RG656BD\3_8     2013-05-02    7 public          192.168.1.254
SNMP iMG606BD\3_8    2013-05-02    7 public          192.168.1.254
SNMP iMG616W\3_8     2012-04-24    7 public          192.168.1.254
SNMP iMG634B_R2\3_8  2012-06-04    7 public          192.168.1.254
SNMP iMG746MOD\3_8   2012-01-31    7 tim123          192.168.1.254

CWMP eDM1405\4_3     2013-05-14    7 public          0.0.0.0         10.52.18.216
CWMP iMG1405W\4_3    2013-04-18    7 public          0.0.0.0         10.52.18.216
CWMP iMG1405W\4_3_108 2013-04-02    7 public          0.0.0.0         10.52.18.216
CWMP iMG1405\4_2_1   2012-11-08    7 public          0.0.0.0         10.52.18.216
CWMP iMG1405\4_2_2   2012-12-05    7 public          0.0.0.0         10.52.18.216
CWMP iMG1405\4_3     2013-04-18    7 public          0.0.0.0         10.52.18.216
CWMP iMG1405\4_3_108 2013-04-02    7 public          0.0.0.0         10.52.18.216
CWMP iMG1405\4_3_84  2013-02-28    7 public          0.0.0.0         10.52.18.216
CWMP iMG1405\4_3_98  2013-03-13    7 public          0.0.0.0         10.52.18.216
```

FIGURE 21-1 iMG Boot Load Configurator - Summary tab

21.4.3 Release 2 and Release 3

The **Release 2** and **Release 3** tabs create loads for iMGs running software release 2-x and 3-x. The **Messages** area displays the processing log.

On the **Release 2** tab, the **Configuration Type** drop-down list contains a list of devices that support software release 2-x. On the **Release 3** tab, the **Configuration Type** drop-down list contains a list of devices that support release 3-x.



Mgmt VLAN ID:

Read Community: public

R/W Community: friend

Trap Host:

Release Load File:

Recovery Load File:

New Load Name:

Configuration Type: RG613 (Rel. 2-X)

TFTP Discovery: ● Disabled ○ Enabled

FIGURE 21-2 iMG Boot Load Configurator Tool - Release 2 and Release 3 tabs

TABLE 21-3 iMG Boot Load Configurator - Release 2 and Release 3 Tabs

Attribute	Value
Mgmt VLAN ID	The VLAN identifier that will be placed into the configuration file. This is the final RG Mgmt VLAN that the RG will use while it is in service for a particular customer in a particular access island. (If the same customer moves and takes the RG it will not work if the new residence is not serviced from the same Access Island. The RG must go through bootstrap again and then it will work again.) Note that this can be the same for all Access Islands, as long as the SNMP Community values are the same (see below).
Read Community	the read SNMP community (default public) that will go into snmpinit. Note: snmp community strings for all iMG/RG should be the same for the entire network.

TABLE 21-3 iMG Boot Load Configurator - Release 2 and Release 3 Tabs

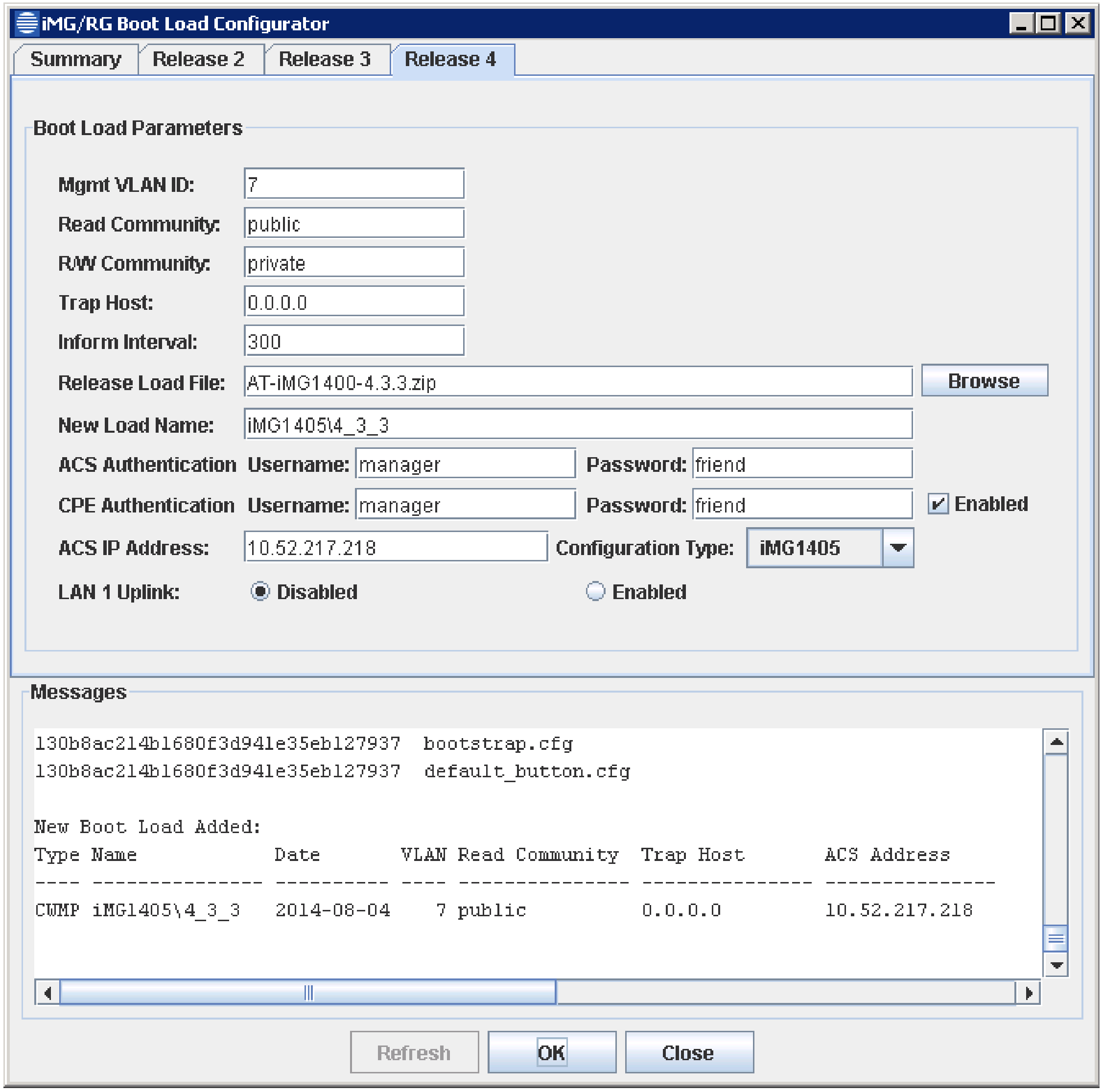
Attribute	Value
R/W Community	the read/write SNMP community (default friend) that will go into snmpinit. Note: snmp community strings for all iMG/RG should be the same for the entire network.
Trap Host	The SNMP trap host (default none) that will go into snmpd.cnf. This will allow configuring multiple trap destination IP addresses separated by a comma. Multiple IP addresses should only be used when creating boot configuration for devices that support it.
Release Load File	This is the zip file that will be unpacked from the NMS's built-in RG/iMG software repository. The files are named after their releases. The Browse button pops up a file chooser from the software repository. (The path of the software repository will be displayed in the beginning of the Messages window)
Recovery Load File	Another zip file, like the release load file, but contains the recovery software, which will also be unpacked from the software repository.
New Load Name	This is the name of the directory path that will be added to the TFTP server directory to contain the new load. The TFTP root path will be displayed in the beginning of the Messages window. Names should not begin with a slash since these directories will be placed under the TFTP root. Subdirectories relative to the TFTP root can be specified by including slashes in the name. (Forward slashes work on both Windows and Linux, but backslashes only work on Windows) If the directory already exists, its contents will be overwritten (after user confirmation), which can be used for correcting mistakes. (In the example, for ADSL iMG/RGs the path could be ADSL/AI01.) The load name must match what is in dhcpd.conf (refer to DHCP Server File (dhcpd.conf)).
Configuration Type	This specifies which type of configuration file to use in the new load. There is a pull-down for devices for the user to select when creating the correct configuration for that release. The Configuration Type drop-down list is confined to devices supported on that software release. On the Release 2 tab, the list contains devices that support software release 2-x. On the Release 3 tab, devices that support software release 3-x are listed.
TFTP Discovery	When selected, after the RG reboots it sends a DHCP discovery message to the DHCP server (over the RGMgmt VLAN). The iMG/RG then sends a tftp request to the NMS, containing its MAC and IP address. The NMS uses its tftp listener to discover the iMG/RG with this IP and MAC Address. With the IP and MAC Address, the AlliedView NMS can proceed with discovery and provisioning.
Messages	Messages show the progress and status of each load creation, including any processing errors. The initial messages include the path to the software repository (where the zip files reside), the path to the TFTP server root (where the loads will be placed), and a summary of any existing loads already residing in the TFTP directory tree. All messages should be reviewed carefully.
Refresh	Only valid for the Summary tab.

TABLE 21-3 iMG Boot Load Configurator - Release 2 and Release 3 Tabs

Attribute	Value
OK	The OK button creates the load from the parameters entered and also creates a new MD5SUM file for all the files in the load. After successfully creating one load, additional loads can be creating by editing the parameters and selecting OK repeatedly. Not applicable to the Summary tab.
Close	Exits the tool. All messages from the Messages window will be saved to a log file in the logs directory (logs/boot_configurator.txt). If the log file gets too big, the oldest entries will be deleted from the log. If, for some reason, saving the log should fail, the user will be prompted to exit anyway or not, and will have a chance to at least copy and paste the contents of the Messages window for future reference, if necessary.

21.4.4 Release 4

The **Release 4** tab is for iMG 1000 and iMG 2000 series devices.



Mgmt VLAN ID: 7

Read Community: public

R/W Community: private

Trap Host: 0.0.0.0

Inform Interval: 300

Release Load File: AT-iMG1400-4.3.3.zip

New Load Name: iMG1405\4_3_3

ACS Authentication Username: manager Password: friend

CPE Authentication Username: manager Password: friend ☑ Enabled

ACS IP Address: 10.52.217.218 Configuration Type: iMG1405

LAN 1 Uplink: ● Disabled ○ Enabled

```
130b8ac214b1680f3d941e35eb127937  bootstrap.cfg
130b8ac214b1680f3d941e35eb127937  default_button.cfg

New Boot Load Added:
Type Name            Date       VLAN Read Community  Trap Host       ACS Address
---- --------------- ---------- ---- --------------- --------------- ---------------
CWMP iMG1405\4_3_3   2014-08-04    7 public          0.0.0.0         10.52.217.218
```

FIGURE 21-3 iMG Boot Load Configurator - Release 4 tab

TABLE 21-4 iMG Boot Load Configurator - Release 4 Tab

Attribute	Value
Mgmt VLAN ID	The VLAN identifier that will be placed into the im.conf file. This is the final RGMgmt VLAN that the RG will use while it is in service for a particular customer in a particular access island. (If the same customer moves and takes the RG it will not work if the new residence is not serviced from the same Access Island. The RG must go through bootstrap again and then it will work again.) Note that this can be the same for all Access Islands, as long as the SNMP Community values are the same (see below).
Read Community	The read SNMP community (default public) that will go into snmpinit. Note: snmp community strings for all iMGs should be the same for the entire network.

TABLE 21-4 iMG Boot Load Configurator - Release 4 Tab

Attribute	Value
R/W Community	The read/write SNMP community (default friend) that will go into snmpinit. SNMP community strings for all iMGs should be the same for the entire network.
Trap Host	The SNMP trap host (default none) that will go into snmpd.cnf. This allows configuring multiple trap destination IP addresses separated by a comma. Multiple IP addresses should only be used when creating boot configuration for devices that support it.
Inform Interval	TR69 inform interval - the interval at which the iMG checks for updates. The default is 300 seconds (5 minutes). This value is used by the iMG only in the bootstrap configuration. When the NMS provisions the iMG, the NMS may set the TR69 inform interval on the iMG to 24 hours.
Release Load File	The zip file that will be unpacked from the NMS's built-in iMG software repository. The files are named after their releases. The Browse button pops up a file chooser from the software repository. (The path of the software repository will be displayed in the beginning of the Messages window)
New Load Name	This is the name of the directory path that will be added to the TFTP server directory to contain the new load. The TFTP root path will be displayed in the beginning of the Messages window. Names should not begin with a slash since these directories will be placed under the TFTP root. Subdirectories relative to the TFTP root can be specified by including slashes in the name. (Forward slashes work on both Windows and Linux, but backslashes only work on Windows) If the directory already exists, its contents will be overwritten (after user confirmation), which can be used for correcting mistakes. (For example, the path could be iMG1405\4_3_3.) The load name must match what is in dhcpd.conf (refer to DHCP Server File (dhcpd.conf))
ACS Authentication	Username and Password iMGs will use to connect to the Auto Configuration Server (ACS).
CPE Authentication	Username and Password ACS will use to connect to iMGs.
ACS IP Address	Normally this is the NMS server IP. If the server has more than one IP, this will be a drop down list.
Configuration Type	This specifies which type of bootstrap file to use in the new load. This is a pull-down for devices for the user to select when creating the correct configuration for that release. This is because some of the releases do not use a configuration compatible to other releases of same type.
LAN 1 Uplink	Enables or disables uplink functionality on the LAN 1 interface. When the uplink is enabled, the LAN 1 interface functions as the WAN interface for the iMG. The LAN interface takes the place of the WAN interface for management and all services are provided over the LAN interface.
Messages	Messages show the progress and status of each load creation. The initial messages include the path to the software repository (where the zip files reside), the path to the TFTP server root (where the loads will be placed), and a summary of any existing loads already residing in the TFTP directory tree. All messages should be reviewed carefully per the cautionary note stated above. Errors will be reported here, as well.
Refresh	Only valid for the Summary tab.

TABLE 21-4 **iMG Boot Load Configurator - Release 4 Tab**

Attribute	Value
OK	The OK button creates the load from the parameters entered and also creates a new MD5SUM file for all the files in the load. After successfully creating one load, additional loads can be creating by editing the parameters and selecting OK repeatedly. Not applicable to the Summary tab.
Close	Exits the tool. All messages from the Messages window will be saved to a log file in the logs directory (logs/boot_configurator.txt). If the log file gets too big, the oldest entries will be deleted from the log. If, for some reason, saving the log should fail, the user will be prompted to exit anyway or not, and will have a chance to at least copy and paste the contents of the Messages window for future reference, if necessary.

21.5 DHCP Server File (dhcpd.conf)

On the DHCP server is the file dhcpd.conf, which includes the options associated with the specific VLAN in the DHCP message. Following is a sample. Refer to Appendix 31. dhcpd Files for a complete example.

Note: The global option specifying the TFTP server, which needs to be set to the NMS ip address, is: option tftp-server-name.)

```
######################################################################
# Class for RGBootStrap for Access Island 01 (AI00) #
######################################################################

class "SPSI-AI00-iMG1525Boot" {

match if ((substring(option agent.remote-id,0,9)="SPSI-AI00")# DHCP RemoteID prefix for iMAPs in AI

and (substring(option agent.circuit-id,2,2)="\x00\xc8") # VLAN 200 See Note 1

and (option vendor-class-identifier = "iMG1525")); # iMG at Release 4 stream

filename "FIBER/AI00/IMG1525"; #<--Directory structure for type of iMG in AI00

option tftp-server-name "10.52.201.4"; #<--IP address of TFTP Server (NMS)

option vendor-class-identifier "iMG1525";

}

class "SPSI-AI00-RG634ABoot" {

match if ((substring(option agent.remote-id,0,9)="SPSI-AI00")

and (substring (option agent.circuit-id,2,2)="\x00\xC8")

and (option vendor-class-identifier="RG634A")); # iMG at Release 3 stream

filename "ADSL/AI00/RG634"; #<--Directory structure for type of iMG in AI00

option tftp-server-name "10.52.201.4"; #<--IP address of TFTP Server (NMS)

option vendor-class-identifier "RG634A";

}
```

Note 1: The VLAN VID is in decimal and the value in the DHCP server in this example mst be in HEX, i.e.:

- 200 = C8 for TEST, so string is "\x00\xC8"
- 201 = C9 for AI01, so string is "\x00\xC9"

- 300 = 12C for TEST, so string is"\x01\x2C"

- 301 = 12D for AI01, so string is"\x01\x2D"

- 400 = 190 for TEST, so string is"\x01\x90"
- 401 = 191 for AI01, so string is "\x01\x91"

- 500 = 1F4 for TEST, so string is"\x01\xF4"
- 501 = 1F5 for AI01, so string is"\x01\xF5"

- 600 = 258 for TEST, so string is "\x02\x58"
- 601 = 259 for AI01, so string is "\x02\x59"

You need a class defined for all the iMG/RG types expected/planned to be used in each Access Island in the network.

The above example shows that when the message comes in over VLAN 200 (usually the bootstrap VLAN for the RG for this Access Island), there is a pointer to the TFTP IP address and a bootstrap filename. If the message comes in over VLAN 300 (RGMgmt), there is no pointer to the TFTP IP address with no bootstrap file name.

21.6 DHCP Relay Configured on the iMAPs (VLAN Configuration)

The DHCP Relay configuration in the iMAP associated with the RG must be data filled so that DHCP instances match the correct IP address for the DHCP server and are associated with the correct VLAN.

The iMAP should be provisioned with at least two DHCP relay instances where data service VLANs (like RGBootstrap, RGVoice, Video, Internet VLANs) are in one relay instance (e.g. MAIN) and the management VLAN (e.g. RGMgmt) is in the second instance (called for example MGMT). Each of these instances should be configured to relay to the specific service provider's operational DHCP server(s) supporting option 82. The second DHCP relay instance (MGMT) will be configured to copy to the AlliedView NMS tftp server as well as to the service providers operational DHCP server(s) supporting option 82.

Note: It is good practice to have one DHCP Relay instance for each service, as well as one for MGMT. Refer to the second example.

Following is the example for MAIN.

```
DHCP Instance Name    Mode          Remote ID          Servers
------------------------------     ----------- ----------------------
MAIN            RELAY           SPSI-AI00-MN1X71      10.10.10.1  *(dhcpsvr1)
```

This MAIN relay instance provides relay service for the example VLANs:

- RGBootstrap - 201
- RGVoice - 601
- Internet - 401 (non-UFO)
- InternetUFO - 451 - In most cases the service VLANs should be UFO.
- Video - 501

Following is the example for MGMT.

```
DHCP Instance Name    Mode          Remote ID          Servers
------------------------------     ----------- ----------------------
MGMT              RELAY         SPSI-AI01-MN1X71    10.10.10.2  *(dhcpsvr2)
                                        10.10.11.1  * (NMS)
```

This MGMT relay instance provides relay service for the example VLAN:

- RGMgmt - 301 - Note that the RGMgmt VLAN must have its own instance.

Note: TLS services should not have DHCP relay enabled for the customer's VPN TLS VLAN. Also, the QoS policy should use classifiers/filters to allow and remark packets appropriately.

Following is an example with one Relay instance per service.

```
DHCP Instance Information

-------------------------

  DHCP Instance  Mode   CID Format      Shelf ID         Remote ID     VLAN

     Name                                          Vid
                                               list
--------------- ----- ------------ ---------------- ---------------- -------
     MAIN      RELAY     AUTO     00:0C:25:1F:80:10 00:0C:25:1F:80:10 None
    RGBoot      RELAY     AUTO     00:0C:25:1F:80:10 SPSI-AI00-MAP5x4  200
    RGMgmt      RELAY     AUTO     00:0C:25:1F:80:10 SPSI-AI00-MAP5x4  300
    RGVoice     RELAY     AUTO     00:0C:25:1F:80:10 SPSI-AI00-MAP5x4  400
   Internet    RELAY     AUTO     00:0C:25:1F:80:10 SPSI-AI00-MAP5x4  600
     Video     RELAY     AUTO     00:0C:25:1F:80:10 SPSI-AI00-MAP5x4  500
-----------------------------------------------------------------------------
```

The iMAP should be provisioned with a unique DHCP “Remote ID” so that the DHCP server can clearly identify where DHCP messages are coming from. Refer to Naming Conventions to Identify Components (DNS) for an overview of naming conventions that should be followed so that administrators can easily label and configure the iMG/RG configuration.

Caution: Ensure that DHCP Relay is enabled on the iMAP network (upstream) interfaces, as well as the interfaces to the iMG/RG. Otherwise, DHCP will not work.

Note: For each Access Island, a unique RGMgmt VLAN and subnet must be provided. All DHCP-related configurations for each Access Island are placed in separate configuration files. SInce each file must declare shared networks, all iMAPs (relay agents) that are in the same Access Island must be declared in the same configuration file. (Includes are supported by dhdpd configuration.) Refer to the Appendix for an example.

21.7 DHCP Relay Configured on the AlliedWare Plus Devices (VLAN Configuration)

The DHCP Relay configuration in the AW+ devices associated with the iMG must be data filled so that the DHCP/VLAN configuration matches the correct IP address for the tftp server and is associated with the correct VLAN.

Here is an example of the config required for dhcp relay on aw+ for the service, rgboot, and rgmgmt vlans:

```
interface vlan201                    //rgboot

ip address 10.52.110.177/28

ip dhcp-relay agent-option

ip dhcp-relay information policy replace

ip dhcp-relay server-address 10.52.201.36

!

interface vlan301                    //rgmgmt

ip address 10.52.110.193/28

ip dhcp-relay agent-option

ip dhcp-relay information policy replace

ip dhcp-relay server-address 10.52.201.36

ip dhcp-relay server-address 10.52.201.4

!

interface vlan401                   //rgvoice
```

```
ip address 10.52.110.209/28
ip dhcp-relay agent-option
ip dhcp-relay information policy replace
ip dhcp-relay server-address 10.52.201.36
!
interface vlan501                    //video
ip address 10.52.110.225/28
ip igmp
ip igmp querier-timeout 1
ip igmp query-max-response-time 1
ip igmp query-interval 25
ip igmp version 2
no ip igmp source-address-check
ip pim dr-priority 100
ip pim sparse-mode passive
ip dhcp-relay agent-option
ip dhcp-relay information policy replace
ip dhcp-relay server-address 10.52.201.36
!
interface vlan601                  //internet
ip address 10.52.110.241/28
ip dhcp-relay agent-option
ip dhcp-relay information policy replace
ip dhcp-relay server-address 10.52.201.36
!
```

Note: *Customers on each switch must be in non-shared subnets, because the AlliedWare Plus devices do standard DHCP Relay with option 82 as circuit ID only (no remote ID) and do not perform DHCP Snooping.*

21.8 Detailed steps for DHCP Discovery

Refer to Figure 21-4 for the first four steps for DHCP discovery.

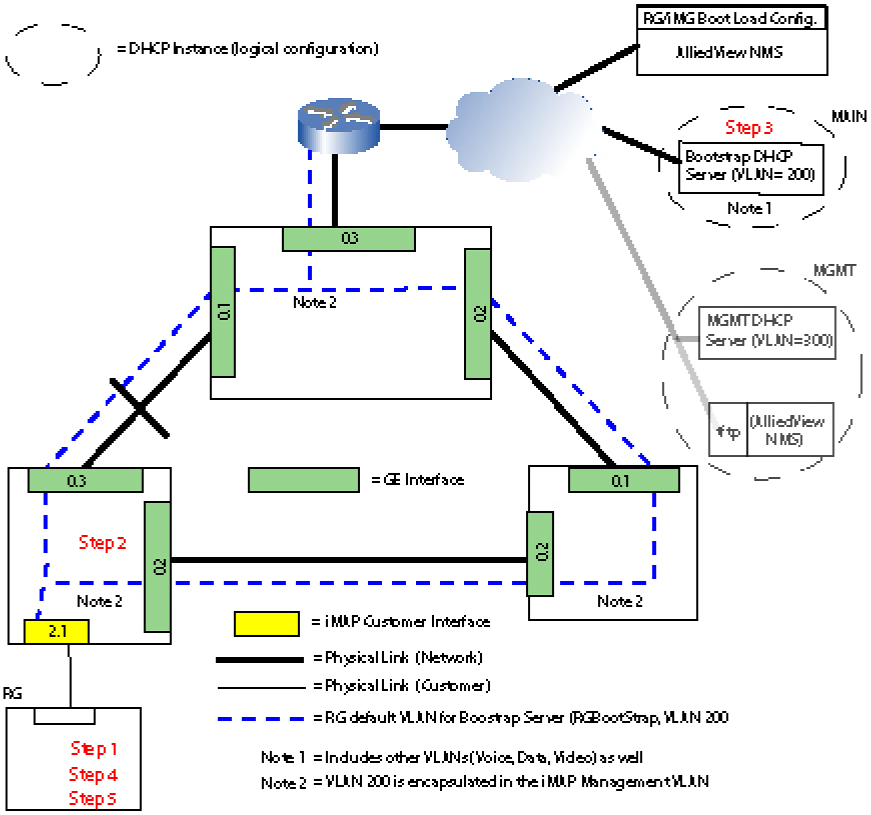

= DHCP Instance (logical configuration)
RG/iMG Boot Load Config.
AlliedView NMS
MAIN
Step 3
Bootstrap DHCP Server (VLAN= 200)
Note 1
MGMT
MGMT DHCP Server (VLAN=300)
tftp
(AlliedView NMS)
03
01
02
Note 2
= GE Interface
03
02
Step 2
Note 2
2.1
01
02
Note 2
= iMAP Customer Interface
= Physical Link (Network)
= Physical Link (Customer)
= RG default VLAN for Boostrap Server (RGBootStrap, VLAN 200
RG
Step 1
Step 4
Step 5
Note 1 = Includes other VLANs (Voice, Data, Video) as well
Note 2 = VLAN 200 is encapsulated in the iMAP Management VLAN

FIGURE 21-4 DHCP Discovery - Bootstrap VLAN

1. The RG powers up and sends a DHCP discover message over the untagged VLAN for its port.
2. The iMAP adds the Remote ID, slot.port, and VID information to the circuit ID and forwards the DHCP discover message to the DHCP server over the inband iMAP Management interface. (Neither the RG nor the end user devices need unicast access to the DHCP server as the iMAP is the proxy relay for them.)

Note: *The iMAP is configured with DHCP Relay so that is sends DHCP messages to both Server and Listener along with the circuit ID attributes.*

3. The DHCP server classifies the Discovery and then sends a DHCP offer message with the free IP address allocated for the RG bootstrap, including a mask, the boot directory, the gateway, the vendor class ID, and the tftp server address of the AlliedView NMS. (As noted, the DHCP server has been configured to know the tftp address.)
4. The RG requests the MD5SUM file from the tftp server, and compares the checksum of its files versus those in the MD5SUM (with its list of files and checksum). The RG performs a GET on any files that differ, as well as the im.conf file that sets up the RGMgmt VLAN using DHCP.

Note: *The recovery code is updated first if needed. (*.rec), then the RG reboots and starts again. Then as needed the main image code and basic "bootstrap" configs elements for the given access island are loaded.*

5. The RG reboots and makes a DHCP discover message to the DHCP server, but this time over the RGMgmt VLAN.

Note: *When an RG is de-provisioned and removed from the server (when customer moves) the RG must be set back to factory. This can be done using the console "sys conf set factory" command or the tic box on the Deprovision Ports form.*

Refer to Figure 21-5 for the next steps for DHCP discovery.

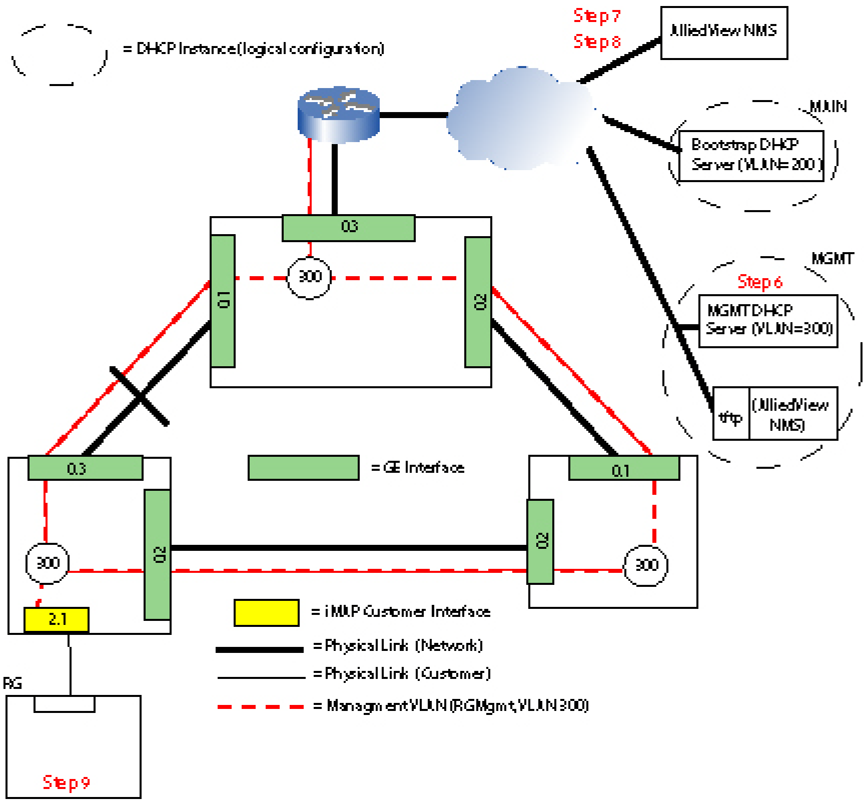

= DHCP Instance (logical configuration)
Step 7
Step 8
AlliedView NMS
MAIN
Bootstrap DHCP Server (VLAN=200)
MGMT
Step 6
MGMT DHCP Server (VLAN=300)
tftp
(AlliedView NMS)
03
300
01
02
03
02
= GE Interface
01
02
300
300
2.1
= iMAP Customer Interface
= Physical Link (Network)
= Physical Link (Customer)
= Managment VLAN (RGMgmt, VLAN 300)
RG
Step 9

FIGURE 21-5 DHCP Discovery - Management VLAN

6. The DHCP server provides the new IP address.
7. The AlliedView NMS uses DHCP Listener to discover the RG (its IP, and Circuit ID attributes such as MAC) in the RGMgmt VLAN.
8. The AlliedView NMS telnets to the RG, and using CLI it configures the RG and saves this to FLASH on the RG.
9. The user should then connect the LAN devices.

Note: *At this point, the RG can provide service if it has been already been pre-provisioned using the Triple Play Customer form. (This form is made easy to fill out if iMG/RG and port profiles have already been defined.) This information is then downloaded to the device and so service can begin. The user has the option, however, to not pre-provision the Triple Play customer form. In this case, the RG is not ready to provide service; the user fills out the form and puts the RG into service once the form is filled out and applied.*

Once the AlliedView NMS has this information, it can create an iMG/RG icon on the AlliedView NMS. Note that the RG is not included on the Physical Map, but in the RG's subnetwork. The RG is also placed in the Network Inventory view under iMG/RGs, and includes the slot.port of its upstream iMAP.

Note: *The Management IP address of the discovered iMG/RG is listed on the Network Inventory table. If the iMG/RG sends traps with a source IP address which is not the Management IP address, the resulting alarm will display this IP source and it may not be able to be mapped to the iMG/RG.*

21.8.1 Discovering Voice Subnets (GenBand, MGC Protocol)

When the voice components are provisioned correctly, all components that are part of VoIP communicate with each other so that dial tone comes up when the RG is plugged in and configured for voice. Moreover, the configuration dynamically updates itself, as IP addresses for voice are renewed/changed for the RG. (The user should be able to swap the RG, and after all components are discovered, the RG can communicate with the voice subnet and dial tone is re-established.)

Refer to the following figure, which shows what must be configured and how the process works.

Before VoIP can work, the following must have already been done, or voice service will not work:

1. Profiles have been filled out correctly to support voice service. In particular, in the Voice profile for the RG, the voice domain name must be filled out, and the voice VLAN that is filled in for the RG General profile has already been created. Also, the route to the Genband must be filled out in the RG General Profile if the Genband is on a separate subnet.
2. The Genband (G6, G2) has been provisioned to support voice (Line Profile, Interface Group, CRV)
3. The GenBand has the routing information for the RG; moreover, the routing table in the GenBand must use the BBI interface.
4. On the Triple Play form, the Genband (G6, G2) information for the GenBand (in Step 2) has been filled in for the customer.
5. There is Dynamic DNS (DDNS) between the DHCP server(s) and the DNS server (usually one is reserved only for voice). This is needed since the DNS tables, which correlate the RG's voice IP interface address with the domain name, are updated dynamically.

Note: The Genband/RG configuration can be statically configured, but this is very difficult to maintain administratively since the IP addresses must be tracked/changed manually.

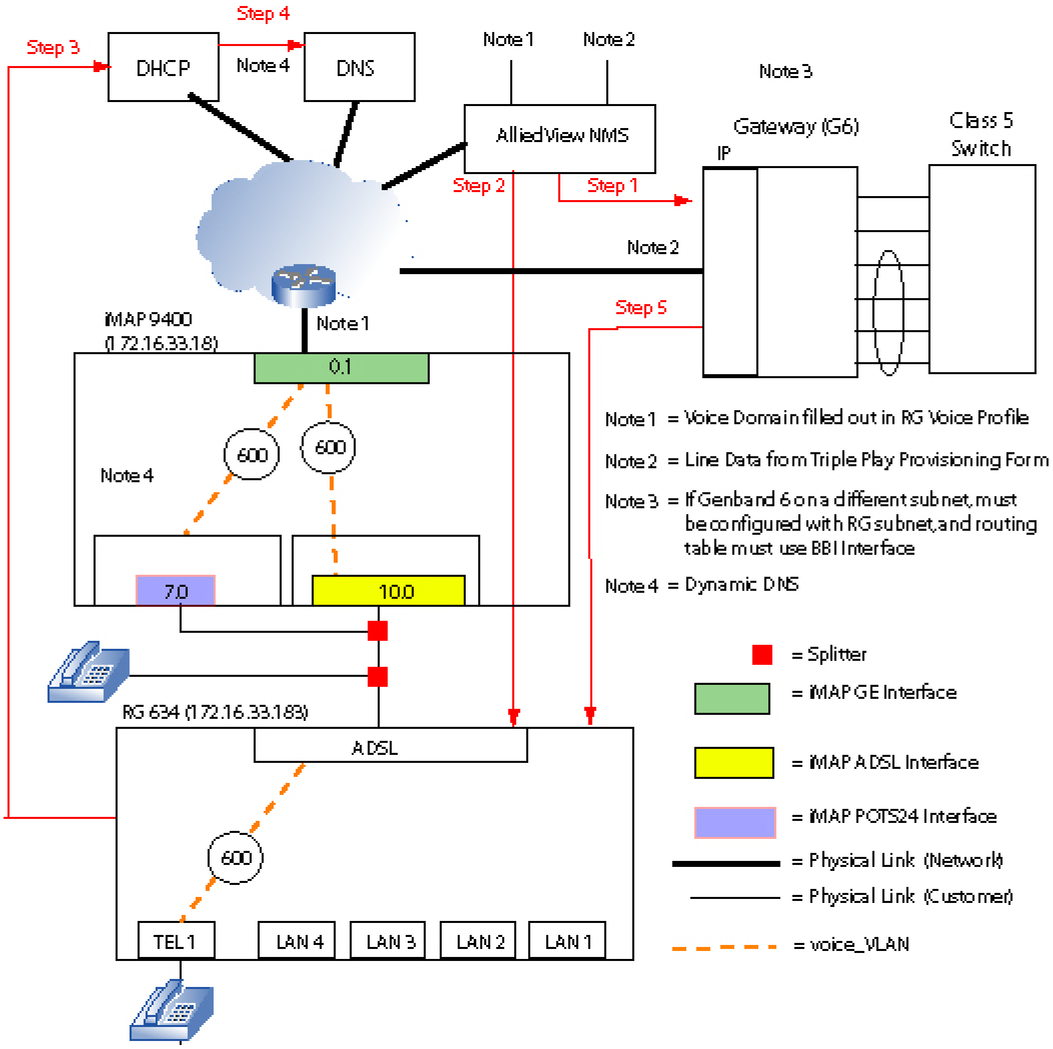


FIGURE 21-6 Voice Service Configuration

When all of the prerequisite steps have been performed and the RG is plugged in, the following occurs:

1. The NMS puts together the FQDN for the RG voice interface (i.e. rgvoip-<MAC addr.>.domain) and the port of the iMAP (as <ip addr of connected iMAP>_slot.port). The AlliedView NMS also adds the line entries that were filled out in the Triple-Play form.
2. The NMS configures each voice line that has been set up for the RG (creates the voice VLAN, creates the voice IP interface, enables DHCP)
3. The RG sends a DHCP discover to the DHCP server. After an exchange of DHCP messages, the DHCP server has the MAC address (sent by the RG) and the IP address (assigned by the DHCP server) associated.
4. The DHCP updates the DNS server to include the DNS entry between the RG's voice IP interface (the rgvoip string) and actual IP address.
5. The MGCP protocol is run between the GenBand and the RG, and the result is a dial tone.

21.9 Naming Convention for Customer IDs (Triple Play Form)

Customer IDs have the following attributes:

- Up to 31 characters in length
- Must be unique so they can identify each customer
- Cannot have wild cards (*)
- Cannot contain the word “error” or “Error”.
- Cannot contain a question mark (?), backslashes (\), double quote (“) or single quote (‘)
- # is allowed

The naming system for customers is entirely up to the administrator, but should reflect one or more of these:

- Specific attributes that identify a customer
- Service mix
- Common attributes when customers form a logical group

Some example IDs could have the format:

- firstname_lastname_phonenumber
- name_servicemix
- name_grouplabel

Note: *This is where a unique prefix (x.) or suffix (_test) would create an easy way to group employees that will participate in ongoing tests but are spread out in many AIs around the network*

Note: *When providing voice service using the G6 (or G2) product, the G6 will drop any characters in the Customer ID after the 20th character. As a result, any customer ID in which the first 20 characters are the same will not be seen as different by the G6. Although customer IDs longer than 20 can be datafilled there will be the following consequences for the provisioned voice lines if the first twenty characters of the Customer IDs are the same:*

- In the Voice Configuration tab of Triple Play Service Management Window, there will be an MGC tab for each voice line that has the identical 20 first characters.

- On the Deprovision Ports Form, multiple voice lines would appear if their associated Customer IDs have the same first twenty characters, and so the administrator would have to know through other attributes the actual voice line(s) to delete.

21.9.1 Changing Customer IDs

Once a Customer ID has been entered using the Triple Play form, it is automatically propagated to the iMG and port-type information, as well as Voice Configuration if the iMG/RG has been configured for voice.

To change the customerID, the administrator must change the customerID for all three types; this is done by changing the CustomerID for all three areas on the Triple-Play Service Management form.

Refer to View/Modify Customer Ports and Changing a Customer ID.

21.10 TR69 Discovery

The NMS can discover iMGs through TR-069 INFORM messages. You should only use TR69 discovery to manage your network where:

- iMGs are not provisioned with the NMS triple play.
- The iMG TR-069 configuration points to the NMS, including the auto configuration server (ACS) URL, the ACS username and password, and the connection request username and password.
- The NMS Discovery Configurator's CWMP configuration matches the iMG TR-069 configuration.
- The network is not using DHCP discovery.

TR69 discovery is disabled by default. You enable it by modifying the `AT_server.properties` file.

21.10.1 Enabling TR69 Discovery

1. Shut down the NMS server.
2. Open the file `<NMS_Home>/conf/AT_server.properties` in a text editor. `<NMS_Home>` is the directory where the NMS is installed.
3. Find the line `TR69_DISCOVERY = FALSE` and change it to `TR69_DISCOVERY = TRUE`.
4. Save and close the file.
5. Start up the NMS server.

The NMS adds the iMGs to the network inventory when it receives the TR-069 INFORM messages. After an iMG is added, subsequent TR-069 INFORM messages from that iMG are ignored.

21.11 Viewing iMGs on the NMS

Once iMGs have been provisioned, you can view them in multiple ways to track their configuration and status.

Figure 21-7 shows the physical node, with the iMAPs grouped according to their Access Island. Note the following:

- The IDs of the iMAPs follow the naming convention explained in Naming Conventions to Identify Components (DNS).
- iMAPs are grouped to show their physical configuration (hub node, ring, links)

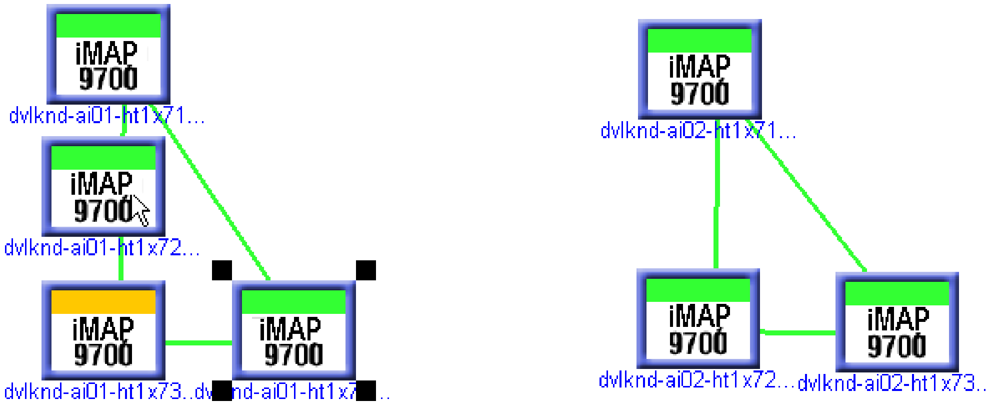
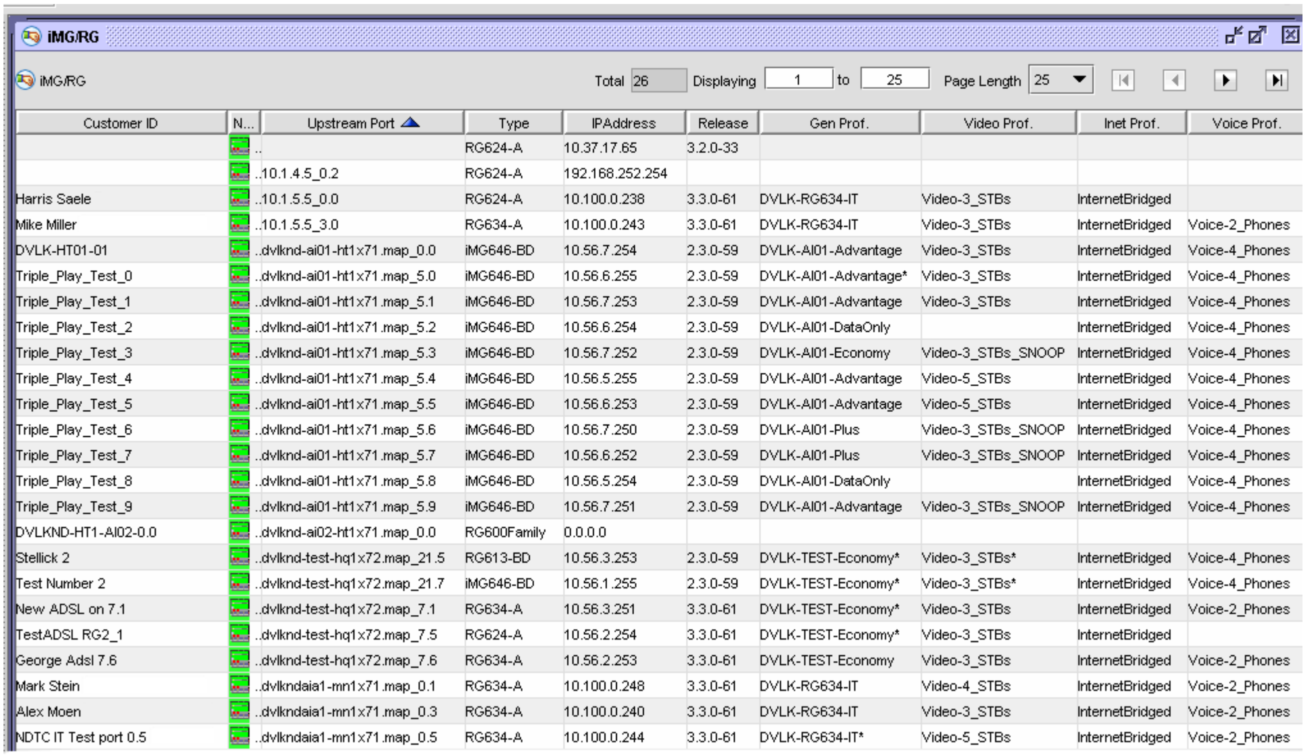


FIGURE 21-7 Physical View - Access Islands

Figure 21-8 shows the RG Inventory List sorted by Upstream port, so the user can easily find specific RG. The table can be sorted by different columns, and the user can create a Custom View to show only specific RGs. (Refer to Creating Custom Views for an Access Island.)



Total 26 Displaying 1 to 25 Page Length 25

Customer ID	N...	Upstream Port ▲	Type	IPAddress	Release	Gen Prof.	Video Prof.	Inet Prof.	Voice Prof.
	🟩	..	RG624-A	10.37.17.65	3.2.0-33				
	🟩	..10.1.4.5_0.2	RG624-A	192.168.252.254					
Harris Saele	🟩	..10.1.5.5_0.0	RG624-A	10.100.0.238	3.3.0-61	DVLK-RG634-IT	Video-3_STBs	InternetBridged	
Mike Miller	🟩	..10.1.5.5_3.0	RG634-A	10.100.0.243	3.3.0-61	DVLK-RG634-IT	Video-3_STBs	InternetBridged	Voice-2_Phones
DVLK-HT01-01	🟩	..dvlknd-ai01-ht1x71.map_0.0	iMG646-BD	10.56.7.254	2.3.0-59	DVLK-AI01-Advantage	Video-3_STBs	InternetBridged	Voice-4_Phones
Triple_Play_Test_0	🟩	..dvlknd-ai01-ht1x71.map_5.0	iMG646-BD	10.56.6.255	2.3.0-59	DVLK-AI01-Advantage*	Video-3_STBs	InternetBridged	Voice-4_Phones
Triple_Play_Test_1	🟩	..dvlknd-ai01-ht1x71.map_5.1	iMG646-BD	10.56.7.253	2.3.0-59	DVLK-AI01-Advantage	Video-3_STBs	InternetBridged	Voice-4_Phones
Triple_Play_Test_2	🟩	..dvlknd-ai01-ht1x71.map_5.2	iMG646-BD	10.56.6.254	2.3.0-59	DVLK-AI01-DataOnly		InternetBridged	Voice-4_Phones
Triple_Play_Test_3	🟩	..dvlknd-ai01-ht1x71.map_5.3	iMG646-BD	10.56.7.252	2.3.0-59	DVLK-AI01-Economy	Video-3_STBs_SNOOP	InternetBridged	Voice-4_Phones
Triple_Play_Test_4	🟩	..dvlknd-ai01-ht1x71.map_5.4	iMG646-BD	10.56.5.255	2.3.0-59	DVLK-AI01-Advantage	Video-5_STBs	InternetBridged	Voice-4_Phones
Triple_Play_Test_5	🟩	..dvlknd-ai01-ht1x71.map_5.5	iMG646-BD	10.56.6.253	2.3.0-59	DVLK-AI01-Advantage	Video-5_STBs	InternetBridged	Voice-4_Phones
Triple_Play_Test_6	🟩	..dvlknd-ai01-ht1x71.map_5.6	iMG646-BD	10.56.7.250	2.3.0-59	DVLK-AI01-Plus	Video-3_STBs_SNOOP	InternetBridged	Voice-4_Phones
Triple_Play_Test_7	🟩	..dvlknd-ai01-ht1x71.map_5.7	iMG646-BD	10.56.6.252	2.3.0-59	DVLK-AI01-Plus	Video-3_STBs_SNOOP	InternetBridged	Voice-4_Phones
Triple_Play_Test_8	🟩	..dvlknd-ai01-ht1x71.map_5.8	iMG646-BD	10.56.5.254	2.3.0-59	DVLK-AI01-DataOnly		InternetBridged	Voice-4_Phones
Triple_Play_Test_9	🟩	..dvlknd-ai01-ht1x71.map_5.9	iMG646-BD	10.56.7.251	2.3.0-59	DVLK-AI01-Advantage	Video-3_STBs_SNOOP	InternetBridged	Voice-4_Phones
DVLKND-HT1-AI02-0.0	🟩	..dvlknd-ai02-ht1x71.map_0.0	RG600Family	0.0.0.0					
Stellick 2	🟩	..dvlknd-test-hq1x72.map_21.5	RG613-BD	10.56.3.253	2.3.0-59	DVLK-TEST-Economy*	Video-3_STBs*	InternetBridged	Voice-4_Phones
Test Number 2	🟩	..dvlknd-test-hq1x72.map_21.7	iMG646-BD	10.56.1.255	2.3.0-59	DVLK-TEST-Economy*	Video-3_STBs*	InternetBridged	Voice-4_Phones
New ADSL on 7.1	🟩	..dvlknd-test-hq1x72.map_7.1	RG634-A	10.56.3.251	3.3.0-61	DVLK-TEST-Economy*	Video-3_STBs	InternetBridged	Voice-2_Phones
TestADSL RG2_1	🟩	..dvlknd-test-hq1x72.map_7.5	RG624-A	10.56.2.254	3.3.0-61	DVLK-TEST-Economy*	Video-3_STBs	InternetBridged	
George Adsl 7.6	🟩	..dvlknd-test-hq1x72.map_7.6	RG634-A	10.56.2.253	3.3.0-61	DVLK-TEST-Economy	Video-3_STBs	InternetBridged	Voice-2_Phones
Mark Stein	🟩	..dvlkndaia1-mn1x71.map_0.1	RG634-A	10.100.0.248	3.3.0-61	DVLK-RG634-IT	Video-4_STBs	InternetBridged	Voice-2_Phones
Alex Moen	🟩	..dvlkndaia1-mn1x71.map_0.3	RG634-A	10.100.0.240	3.3.0-61	DVLK-RG634-IT	Video-3_STBs	InternetBridged	Voice-2_Phones
NDTC IT Test port 0.5	🟩	..dvlkndaia1-mn1x71.map_0.5	RG634-A	10.100.0.244	3.3.0-61	DVLK-RG634-IT*	Video-5_STBs	InternetBridged	Voice-2_Phones

FIGURE 21-8 iMG/RG Inventory View Sorted by Upstream Port

21.12 Provisioning the iMG Managed Object Properties

- Managed Object Properties for the iMG

Object Properties to Define Objects and Custom Views describes all the relevant managed objects and their properties so that the user can control how the MO is provisioned. This is especially helpful in understanding how MO properties can be filtered in Custom Views.

- Custom Views

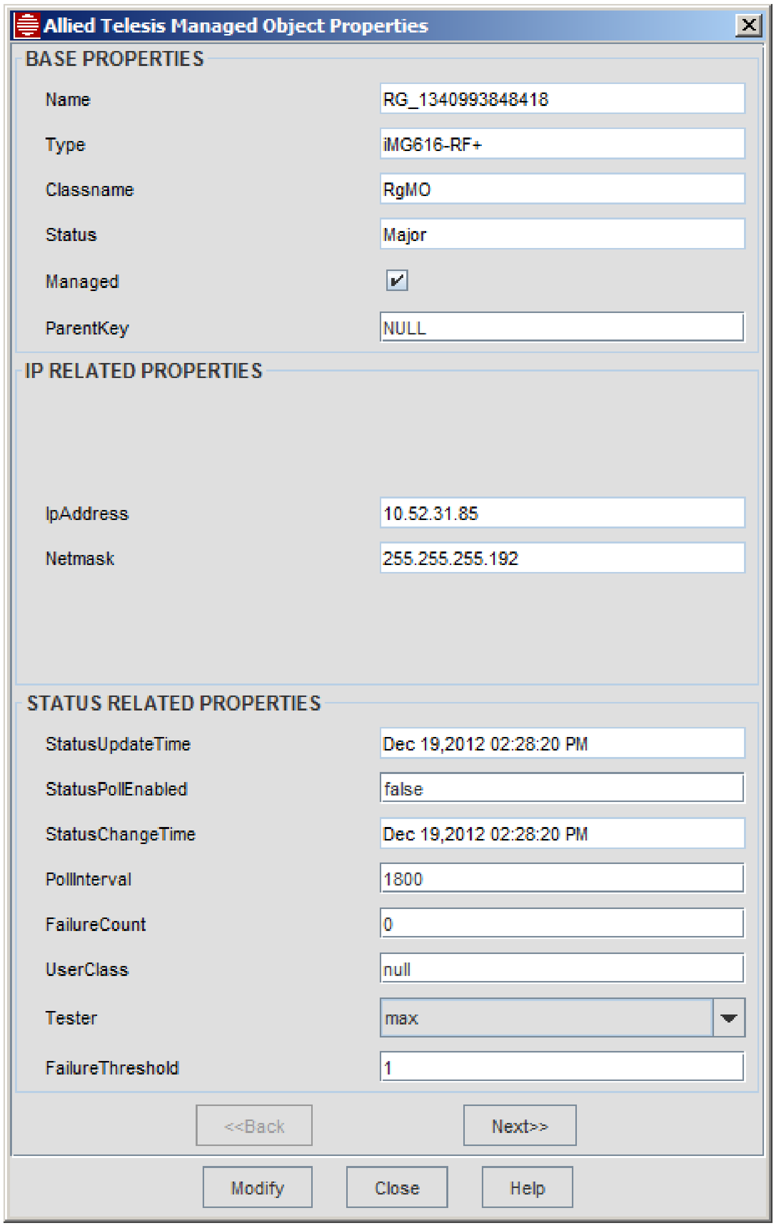
  An Access Island is a group of up to eight iMAPs (with one hub) that are used for a Service Location. In most cases, being able to identify the components specific to an Access Island helps in provisioning current and future subscribers as well as troubleshooting problems.

  The example Custom Views in Creating Custom Views for an Access Island should be created for each Access Island.

21.12.1 Managed Object Properties for the iMG

The following figure and table explain the properties for iMGs and is useful for both provisioning and for creating Custom Views.

Note: For SysName, SysLocation, and SysContact, the NMS checks for up to 255 characters, and outputs a specific error message if more than 255 characters are input. If the device allows a maximum of less than 255 characters, the NMS will still flag the mistake but the error message is a more generic "webserver: Value too long".



Allied Telesis Managed Object Properties

BASE PROPERTIES

Name	RG_1340993848418
Type	iMG616-RF+
Classname	RgMO
Status	Major
Managed	☑
ParentKey	NULL

IP RELATED PROPERTIES

IpAddress	10.52.31.85
Netmask	255.255.255.192

STATUS RELATED PROPERTIES

StatusUpdateTime	Dec 19,2012 02:28:20 PM
StatusPollEnabled	false
StatusChangeTime	Dec 19,2012 02:28:20 PM
PollInterval	1800
FailureCount	0
UserClass	null
Tester	max
FailureThreshold	1

FIGURE 21-9 Managed Object Properties Form for an iMG

TABLE 21-5 Managed Object Properties for Nodes

MO Form Property	Description for Nodes	Custom Map View Property	Example
Name	The device name, which is a unique name that is used as the key in the database. This name cannot be changed.	name	172.16.33.11 or DVLKND-AI01* (sets scope for Access Island 01)
Type	The type of the object, such as whether it is a network, node, or an interface object, or something user specified, like router, switch, etc.	type	9700 9400 Rapier* (all Rapier devices) RG* (all RG devices)
Managed	A checkbox that indicates whether the managed object is managed by the NMS. When checked, the object is being managed by the NMS. Otherwise, it is not.	managed	true (would not include devices that were discovered and unmanaged)
IpAddress	The unique address assigned to each and every object.	ipAddress	172.16.33.11
Netmask	The netmask that is specified for this managed object. Network masking is a methodology by which the elements in a network can be meaningfully categorized.	netmask	255.255.255.0
ParentNet	The ID of the network that contains this node or a list of network numbers if this is a router connecting two or more networks.	parentNet	172.16.33.0
InterfaceList	A non modifiable drop-down list of all interfaces on this device.	InterfaceList	172.16.33.20 172.16.33.21 (The value all would select all nodes.)
Tester	The type of testing to run when checking the status of the device.		
Community	The community string of the corresponding SNMP agent associated with the link	community	
SysName (Internal)	The system name as reported by the SNMP agent		
SysDescr	The value of the system description associated with the type of managed object to be filtered.	sysDesc	Telesis 9700 all
SysOID	The system object identifier of the device as reported by the SNMP agent of the device.	sysOID	.1.3.6.1.4.1.207.1.15.3
Login	The CLI username to use when the NMS executes CLI commands on the device. It is defaulted but it should be changed.	login	officer
Password	The password to use when NMS logs in with the CLI username.		klk3kdr3

TABLE 21-5 Managed Object Properties for Nodes (Continued)

MO Form Property	Description for Nodes	Custom Map View Property	Example
SysLocation	A string value to identify where the device is located	sysLocation	Building_A (This would assume the device was located in Building_A)
Category	The family of the device	category	Telesis (includes all MAP devices) Rapier* (all Rapier devices) RG* (all RG devices)
Release	The release ID of the device software.	release	
InetProfileMOName	The unique DB names of the Internet profiles associated with this RG		
RgGenProfileMOName	The unique DB names of the General profiles associated with this RG		
VoipProfileMOName	The unique DB names of the voice profiles associated with this RG		
VoipProfileName	Display names of the RG Voice profiles currently associated with this RG		
RgGenProfileName	Display names of the RG General profiles currently associated with this RG		
VideoProfileName	Display names of the RG Video profiles currently associated with this RG		
InetProfileName	Display names of the RG Internet profiles currently associated with this RG		
SysContact	A string to identify the owner of the device	sysContact	Company_A
ConfigChanged	The time that a change to the device's configuration has been detected by the Device Backup operation. Config changes will be detected automatically when recurring backups are scheduled. This property is included in the Nodes custom view under the Network Inventory by default.	configChanged	
LastBackupTime	The time of the last backup performed for this device via the Device Backup/Restore MDTI Operation.	lastBackupTime	Wed Aug18 2004*
MacAddr	The MAC Address of the RG		
RgCustomerID	The unique customer ID for the RG		
Source			DVLKND-mgc1* (G6)

Note: The attributes ending in ProfileName are the display names of the profiles currently associated with this RG. The attributes ending in ProfileMOName are the unique DB names of the profiles associated with this RG.

TABLE 21-6 Managed Object Properties for Ports

MO Form Property	Description for Ports	Custom Map View Property	Example
Name	The device name, which is a unique name that is used as the key in the database. This name cannot be changed.	name	172.16.33.11 or DVLKND-AI01* (sets scope for Access Island 01)
Type	The type of the object, such as whether it is a network, node, or an interface object, or something user specified, like router, switch, etc.	type	7700 (Only 7700 would be included Other values are: 9700 9400 (all Rapier devices) RG* (all RG devices)
UpstreamDevicePort	The <Map Name>_slot.port of the port that the RG is connected to.		
SubType			*Gigabit*

21.12.2 Creating Custom Views for an Access Island

When the iMG/RG is first provisioned, it is not included on the Physical Map, but in the RG's subnetwork. The RG is also placed in the Network Inventory view under iMG/RGs, and includes the slot.port of its upstream iMAP.

The network should be divided into Access Islands, each with its hub iMAP and node iMAPS with their subtending iMG/RGs. Starting from the initial views of the iMG/RGs, the network administrator should create Custom Views that highlight the components of an Island. This makes provisioning and monitoring of the Island much easier.

Note: Refer to Object Properties to Define Objects and Custom Views for a listing of all managed object properties that can be used to create custom views and examples.

Note: Do not to use special characters in a view name, or an error will result

Following are the main rules when defining criteria:

- For string-based properties, the string value is absolutely matched. For example, the string "Router" matches the exact word only.
- The wildcard '*' (asterisk) is supported to replace one or more characters. For example, if you want to view objects whose names start with 'sa', then you have to specify it as 'sa*'. Similarly, if you want to view objects whose names end with 'com', then you have to specify as '*com'.
- Wildcard, '?' is not supported and is treated just as an ordinary character.
- For specifying multiple criteria for the same property, separate them with a comma. For example, if you want to view objects named nms-server1, nms-server2 and nms-server3 then specify as nms-server1, nms-server2, nms-server3.
- To exclude certain items, as part of the filtering criteria, append a '!' before it. The exclamation mark should be used to ignore those values. For example, if you want to view objects, which do not start with 's", then specify the property as '!sa*' or if you want to see all Alarms, except those with severity other than warning and clear, then any of the following will work:
- !war*, !cle*
- !warning, !clear

- cr*, maj*, mino*
- critical, major, minor

Click on the **More** button and then **Select Additional Criteria** to include more attributes that will filter this form. Use the exact name for the criteria and follow the rules above. You can also choose Select Props to View to select which fields will appear in the view. (This is different than defining the criteria to filter a view.)

Figure 21-10 shows the AlliedView NMS as it is configured for an Access Island (called AccessIsland_1)

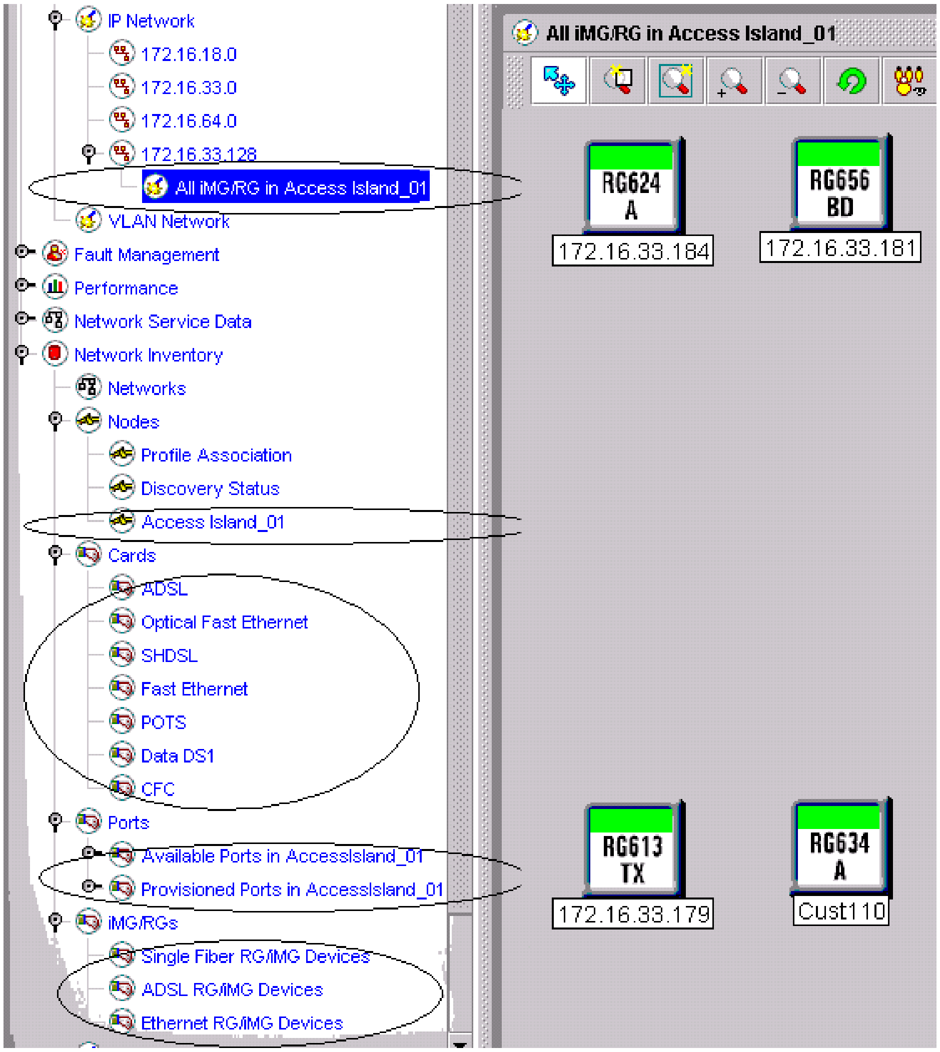


FIGURE 21-10 Custom Views for iMG/RG Management (Access Island 01)

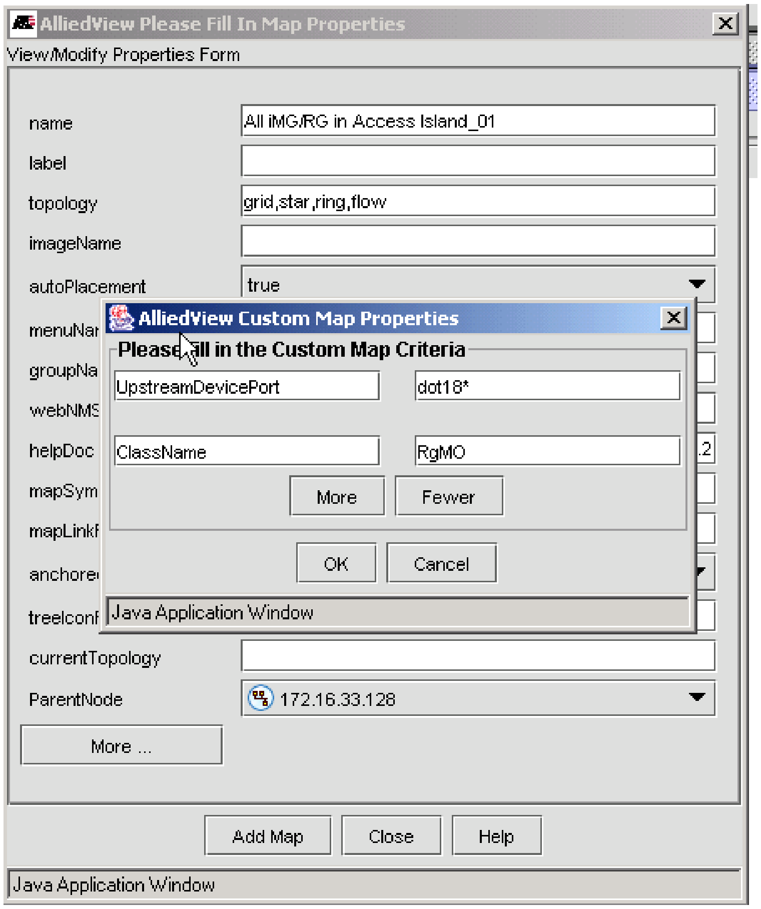
21.12.2.1 All iMGs in an Access Island (in IP Network Map)

As shown in Figure 21-10, there is a Custom Map View for all iMG./RGs for Access Island 1 that shows all iMG/RGs that are part of this Access Island. To create this Custom View, perform the following steps:

1. Select the Network Node that will have the Custom View as a sub-node (this can also be done later).
2. Right click on this Node and select *Custom Views -> Add Custom Map* (or Control-N)
3. On the Map Properties form, fill in the Name you wish to give this Custom Map. (You can also choose the parent node here if you wish to change this.)

4. Click on the **More** button and the Select Additional Criteria to include more attributes that will filter this form. The following figure shows which attributes are used, **ClassName** (RgMO), and **UpstreamDevicePort**, with a criteria that selects all the subtending nodes in the Access Island.

Note: *You must create or "manage" all rgmgmt IP subnets beforehand; The NMS learns of RG's via "DHCP" or "Discover Attached iMG/RG" otherwise they will not show up in the any IP subnet MAP.*


AlliedView Please Fill In Map Properties
View/Modify Properties Form
AlliedView Custom Map Properties
Please fill in the Custom Map Criteria
More
Fewer
OK
Cancel
Java Application Window
More ...
Add Map
Close
Help
Java Application Window

name	All iMG/RG in Access Island_01
label	
topology	grid,star,ring,flow
imageName	
autoPlacement	true
menuNar	
groupNa	
webNMS	
helpDoc	
mapSym	
mapLinkF	
anchore	
treeIconf	
currentTopology	
ParentNode	172.16.33.128

UpstreamDevicePort	dot18*
ClassName	RgMO

FIGURE 21-11 Custom Map for iMG/RGs in an Access Island

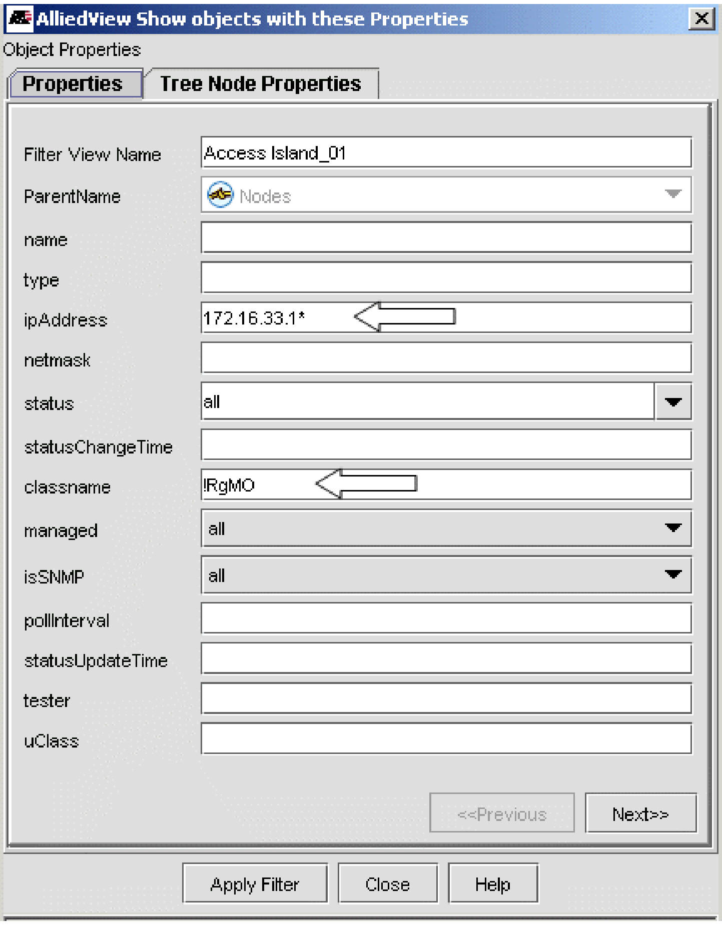
21.12.2.2 All iMAP Nodes in an Access Island

In the Nodes view of Network Directory tree, a Custom View can be created that includes all the iMAPs for an Access Island. To create this Custom View, perform the following steps:

1. Select Nodes under Network Inventory.
2. Right click and select *Custom Views -> Add Custom View* (or Control-V)
3. On the Object Properties form, fill in the Name you wish to give this Custom View. (Note that in this case you cannot choose the parent node.)

Click on the **More** button to include the attributes that will filter this form. The following figure shows which attributes are used, not **classname** (!RgMO), and **ipAddress** (if all iMAPs for the Access Island are in the same subnet), with a criteria that selects all the iMAPs in the Access Island.

Note: *You can click on Name as well, using a name such as DVLKND-AI01* if using the naming convention suggested in this Section.*



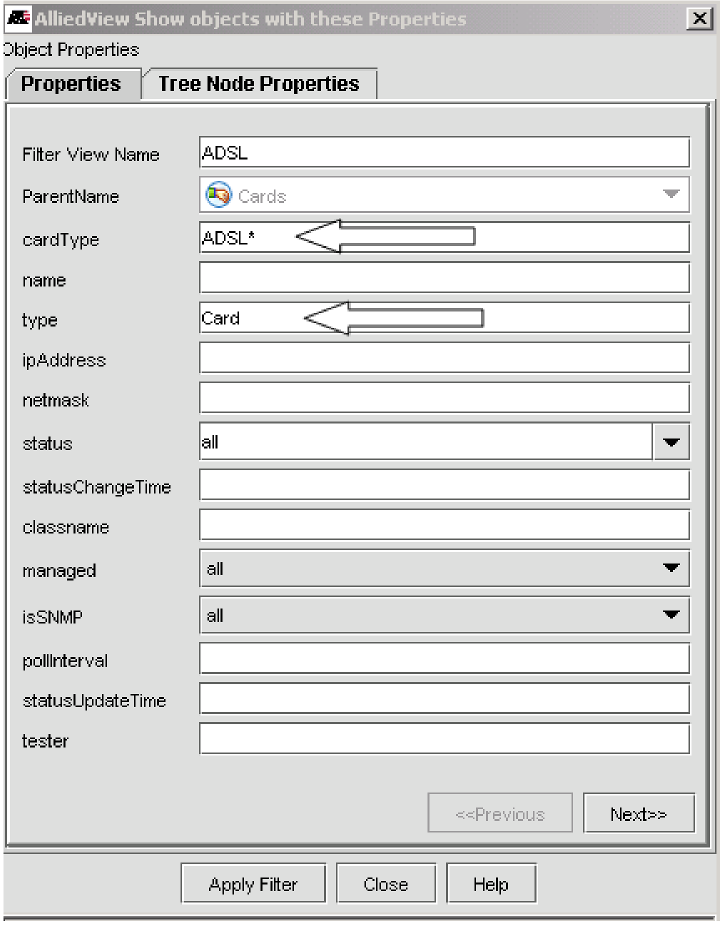
Filter View Name: Access Island_01
ParentName: Nodes
name:
type:
ipAddress: 172.16.33.1*
netmask:
status: all
statusChangeTime:
classname: !RgMO
managed: all
isSNMP: all
pollInterval:
statusUpdateTime:
tester:
uClass:

FIGURE 21-12 Creating a Custom View for all iMAPs in an Access Island

21.12.2.3 iMAP Cards Grouped by Type

To create Custom Views for each card type, create Custom Views with the following filtering criteria.

- ADSL - cardType=ADSL*, type=Card
- Optical Fast Ethernet - cardType = FX*, type=Card
- SHDSL - cardType=SHDSL*, type=Card
- Fast Ethernet - cardType=FE*, type=Card
- POTS - cardType=POTS*, type=Cardtype=Card
- VDSL - cardType=VDSL*, type=Card


AlliedView Show objects with these Properties

Object Properties

Filter View Name: ADSL
ParentName: Cards
cardType: ADSL*
name:
type: Card
ipAddress:
netmask:
status: all
statusChangeTime:
classname:
managed: all
isSNMP: all
pollInterval:
statusUpdateTime:
tester:

FIGURE 21-13 Example Custom View for Card Types

21.12.2.4 Provisioned / Available Ports in an Access Island

In the Ports node, it is useful to create a Custom View for provisioned and unprovisioned ports, since the administrator could then quickly see the pool of unprovisioned ports that could be used for adding subscribers.

For provisioned ports, the filtering criteria is as follows: (names are for an example customer):

- customerID = ! (logical not, since a provisioned port must have a customer ID)
- type = CustPort
- parentKey = dot18*

For available ports, the filtering criteria is as follows:

- ethIfIndex = <> (null, since an available port does not have an Ethernet index value)
- customerID = <> (null, since an available port does not have a customer ID)
- type = CustPort
- parentKey = dot18* (This narrows the view down to the Access Island.)

An example would be a Custom View that showed all GE ports on Access Island 01. The criteria would be:

- name = DVLKND-AI01*
- SubType = *Gigabit*

Note: Sorting or ordering of these views is not supported, so the creation order is important.

1. create a view of all unprovisioned ports
2. Create two views (unprovisioned/provisioned) per Access Island.

21.12.2.5 iMG/RGs Grouped by Type

Custom Views should also be created for the iMG/RG type, allowing the administrator to isolate an iMG/RG and the services it can provide, as well as which RGs have not been provisioned yet. Example criteria is as follows:

- ADSL - className=RgMO, type=iMG6*4*
- Ethernet - className=RgMO, type=!iMG6*4*
- MOD - className=RgMO, type=*MOD*
- Unprovisioned - className=RgMO, rgCustomerID=<> (null, since a provisioned RG must have a Customer ID)
- Voice - className=RgMO, voipProfileName=!

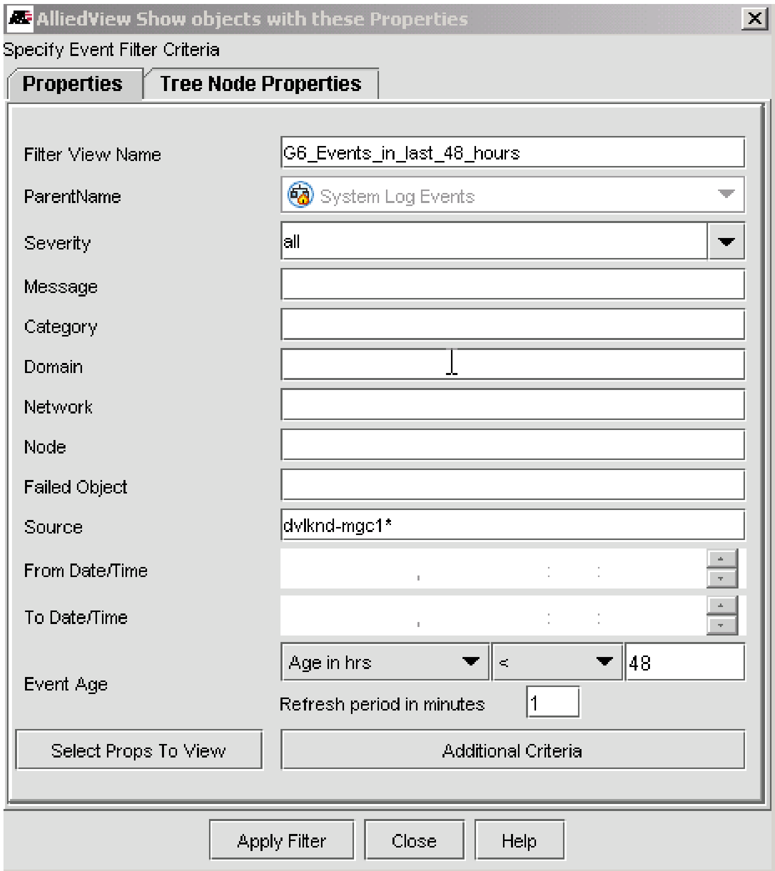
21.12.2.6 Fault Management

Custom Views should also be created for fault conditions or output The filtering criteria is as follows:

- Syslog CLI Events - Category = SYSLOG-CLI*

Note: An alarm category of Battery is available, so these battery-related alarms can easily be viewed in the Alarm Summary View in the main AlliedView NMS screen.

- G6 events in last time period (i.e. 24 hours) - refer to the following figure



AlliedView Show objects with these Properties

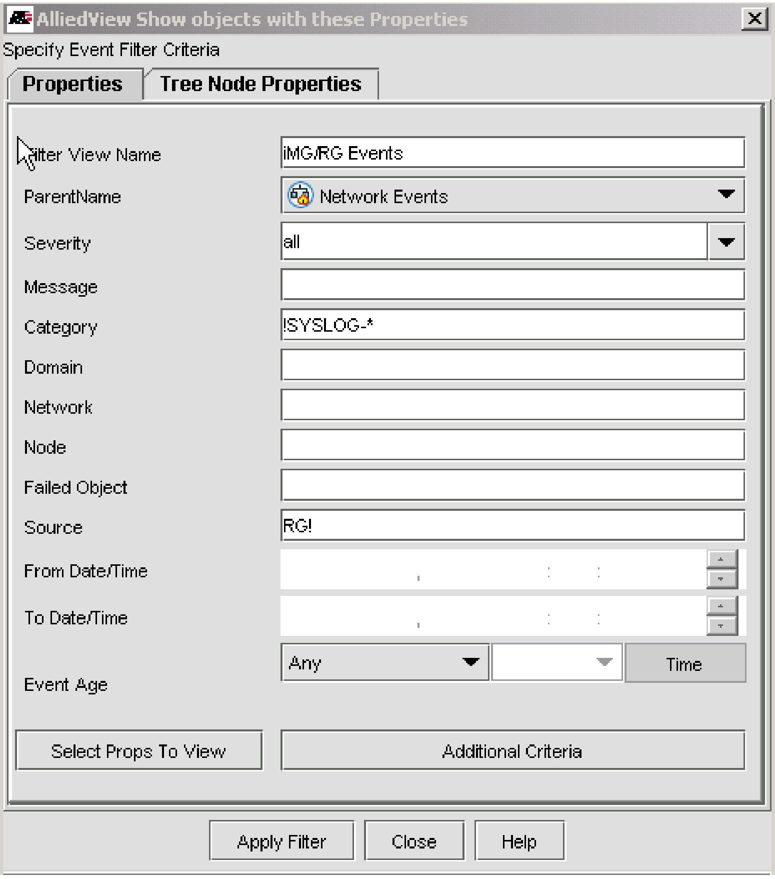
Specify Event Filter Criteria

Filter View Name	G6_Events_in_last_48_hours
ParentName	System Log Events
Severity	all
Message	
Category	
Domain	
Network	
Node	
Failed Object	
Source	dvlknd-mgc1*
From Date/Time	
To Date/Time	
Event Age	Age in hrs < 48

Refresh period in minutes 1

FIGURE 21-14 Custom View for G6 Events in last 48 hours

- All RG/iMG events in the network - Refer to the following figure.


AlliedView Show objects with these Properties
Specify Event Filter Criteria
Properties
Tree Node Properties

Filter View Name: iMG/RG Events
ParentName: Network Events
Severity: all
Message:
Category: !SYSLOG-*
Domain:
Network:
Node:
Failed Object:
Source: RG!
From Date/Time:
To Date/Time:
Event Age: Any

FIGURE 21-15 Custom View for RG/iMG Events

21.13 Provisioning the iMG (Application Manager)

Caution: *If you are accessing applications via an IP route that includes Network Address Translation (NAT), certain modules may not work correctly as the server may send information to the clients over different ports than those initiated by the clients. You should therefore set up an FE on the back side of the NAT or remove the NAT process to prevent this.*

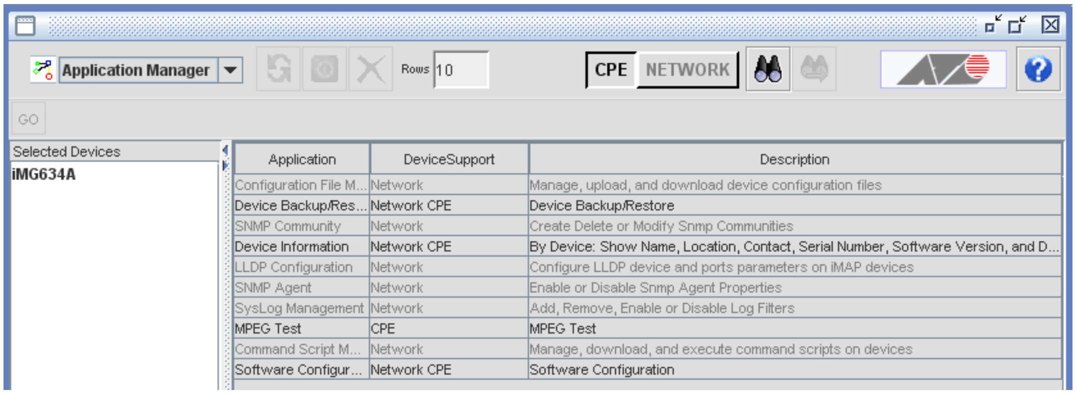
As described in Provisioning a Device, the Provisioning Application for Allied Telesis devices allows you to control software related tasks (backup/restore, command scripting, SNMP, file management, etc.). This same provisioning GUI can be used for the iMGs/RGs as follows:

- The tasks available are Device Backup/Restore, Device Configuration, and Software Configuration
- The GUI has a device type selection button, **NETWORK** and **CPE**, that allows the administrator to choose one type of device or another. This allows the administrator to focus on only one type of device at a time, an important capability since there may be thousands of iMG/RGs and a much smaller number of Allied Telesis devices.

To access the Application Manager:

- Right-click on a device (as an icon or table row), and select *Provision -> (Provisioning Task).*
- From the main menu, select *Tools -> Application Manager.*

The following figure shows the result when the user selects *Tools -> Application Manager.*



Selected Devices
iMG634A

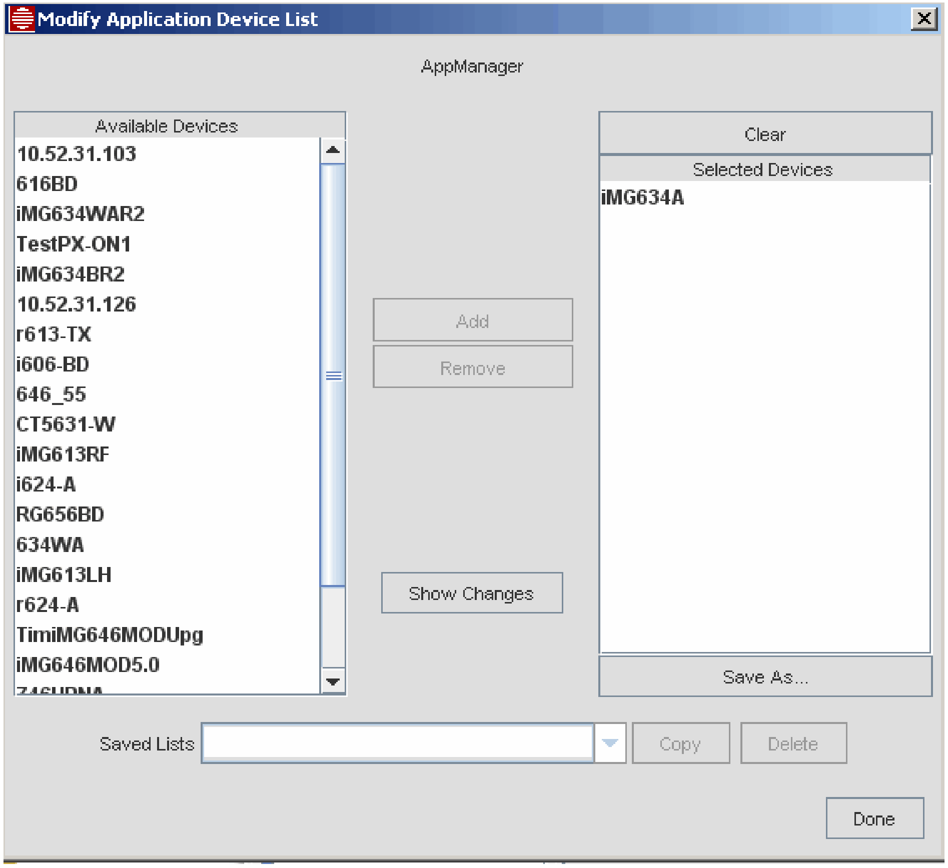
Application	DeviceSupport	Description
Configuration File M...	Network	Manage, upload, and download device configuration files
Device Backup/Res...	Network CPE	Device Backup/Restore
SNMP Community	Network	Create Delete or Modify Snmp Communities
Device Information	Network CPE	By Device: Show Name, Location, Contact, Serial Number, Software Version, and D...
LLDP Configuration	Network	Configure LLDP device and ports parameters on iMAP devices
SNMP Agent	Network	Enable or Disable Snmp Agent Properties
SysLog Management	Network	Add, Remove, Enable or Disable Log Filters
MPEG Test	CPE	MPEG Test
Command Script M...	Network	Manage, download, and execute command scripts on devices
Software Configur...	Network CPE	Software Configuration

FIGURE 21-16 Application Manager GUI for CPE (iMG/RG)

Note that the user can select the CPE button and only the tasks available are highlighted; the others are grayed out. (The others would be available if the user had chosen **NETWORK**.)

The options available are similar to those for network devices. The user can double-click on one of the Applications in the table (or select the application, and then click **GO**) and it will invoke the specific application window.

If the user clicks **Add/Remove Devices**, which is at the bottom of every application window, the set of (CPE) devices that are to be included in the application can be controlled, as shown in the following figure. Refer to Overview of the Provisioning Interface for details on using the buttons and options.



Available Devices
10.52.31.103
616BD
iMG634WAR2
TestPX-ON1
iMG634BR2
10.52.31.126
r613-TX
i606-BD
646_55
CT5631-W
iMG613RF
i624-A
RG656BD
634WA
iMG613LH
r624-A
TimiMG646MODUpg
iMG646MOD5.0

Selected Devices
iMG634A

Saved Lists

FIGURE 21-17 List of CPE Devices available for an Application

21.14 Provisioning Guidelines for Models

This section covers the following models:

- Open Access
- Multi-service VLANs
- iMG6x6MOD/iMG7x6MOD - Translation and HPNA Diagnostics
- iBG915-FX
- iMG with WAN 1G Module
- Split Management for Wireless iMGs
- Changing VoIP Endpoint Syntax
- Provisioning Custom VLANs
- Error Conditions when Provisioning

21.14.1 Open Access

Figure 21-18 shows an example configuration in which there are nine Service Providers, three for each type of service. As a result, there are nine VLANs that exist for these services, and changing a service provider for a service requires a different VLAN to be used.

Do the following to provision the Open Access model:

- Mgmt. Profile - Set the ‘Include VLANs in Profile’ to False - The service VLAN fields are de-activated, since these VLANs are now filled in individual service profiles
- Service Profiles - In the Voice, Video, and Internet profiles, set the ‘Include <service type> VLAN in Profile’ field to True. The service VLANs are activated and can be filled in.

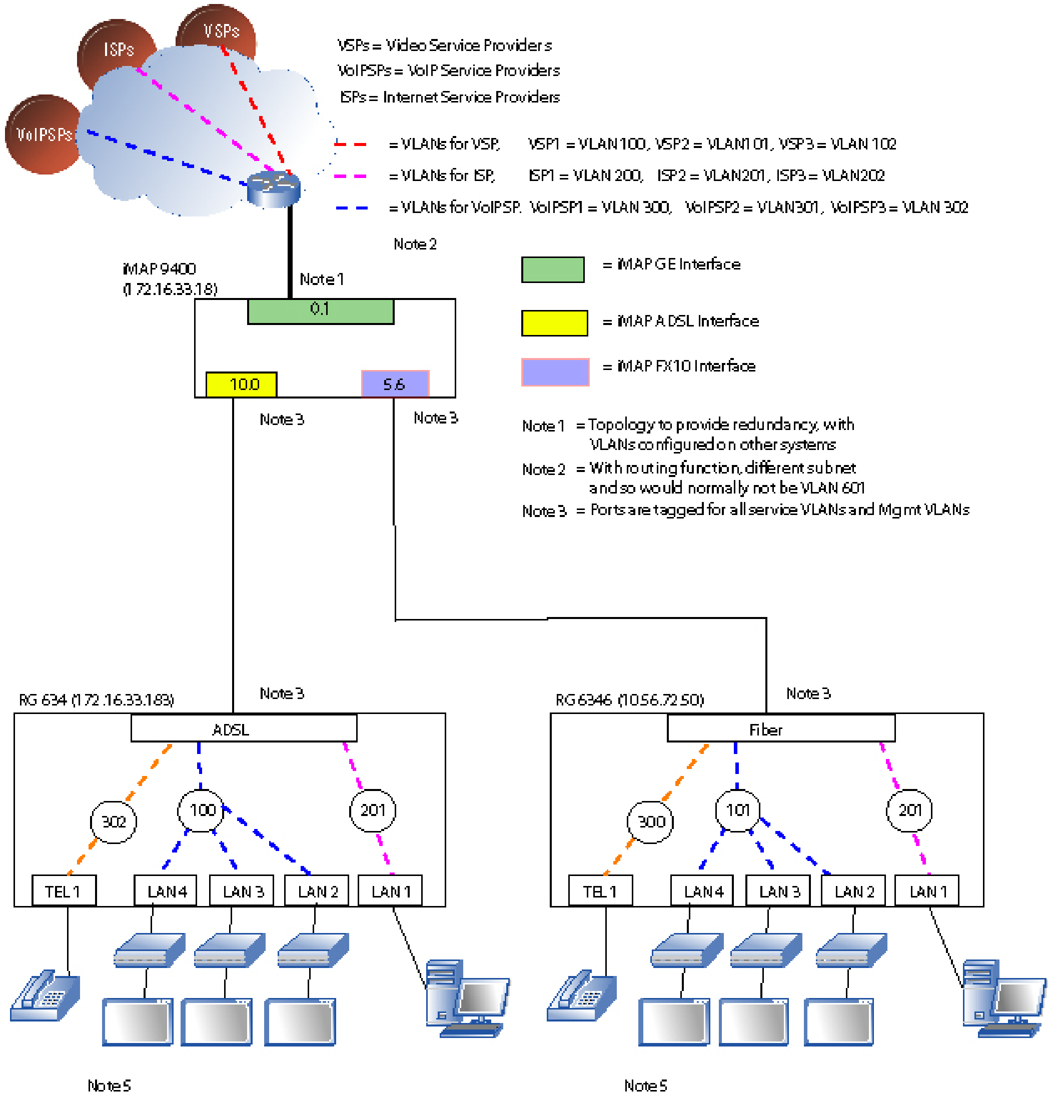
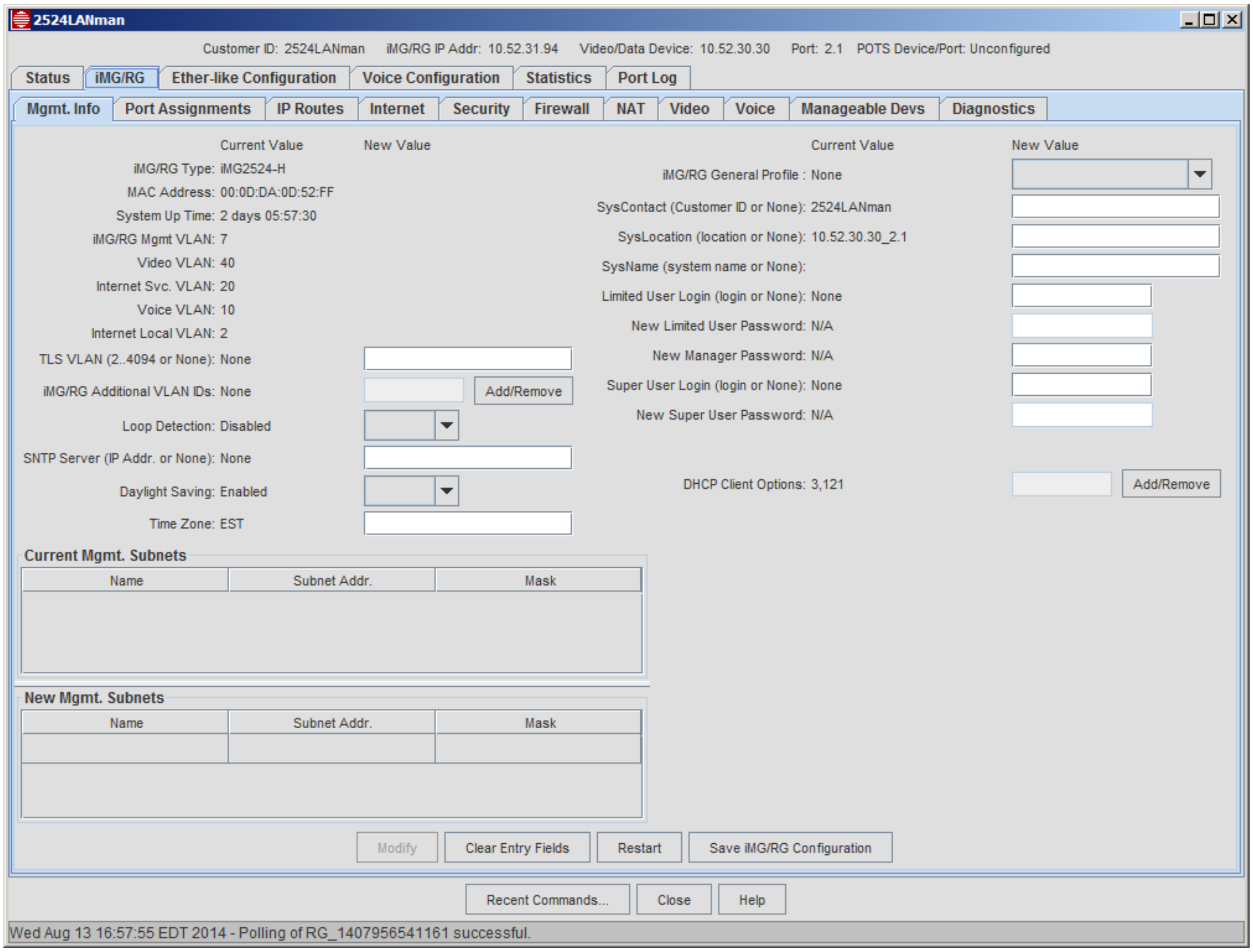

VSPs
ISPs
VoIPSPs
VSPs = Video Service Providers
VoIPSPs = VoIP Service Providers
ISPs = Internet Service Providers
= VLANs for VSP, VSP1 = VLAN 100, VSP2 = VLAN1 01, VSP3 = VLAN 102
= VLANs for ISP, ISP1 = VLAN 200, ISP2 = VLAN201, ISP3 = VLAN202
= VLANs for VoIPSP. VoIPSP1 = VLAN 300, VoIPSP2 = VLAN301, VoIPSP3 = VLAN 302
Note 2
iMAP 9400
(172.16.33.18)
Note 1
0.1
10.0
5.6
🟩 = iMAP GE Interface
🟨 = iMAP ADSL Interface
🟪 = iMAP FX10 Interface
Note 3
Note 3
Note 1 = Topology to provide redundancy, with VLANs configured on other systems
Note 2 = With routing function, different subnet and so would normally not be VLAN 601
Note 3 = Ports are tagged for all service VLANs and Mgmt VLANs
RG 634 (172.16.33.183)
Note 3
ADSL
302
100
201
TEL 1
LAN 4
LAN 3
LAN 2
LAN 1
RG 6346 (10.56.72.50)
Note 3
Fiber
300
101
201
TEL 1
LAN 4
LAN 3
LAN 2
LAN 1
Note 5
Note 5

FIGURE 21-18 iMG/RGs in a Network with Multiple Providers for each Service

Once the Open Access model is configured, the Service Management Form is similar to the Access Island model; on the Mgmt. Info tab, the service VLANs are read only, and so the user must go to the individual service tabs to change a VLAN. Refer to the following figure.



Customer ID: 2524LANman iMG/RG IP Addr: 10.52.31.94 Video/Data Device: 10.52.30.30 Port: 2.1 POTS Device/Port: Unconfigured

	Current Value	New Value
iMG/RG Type:	iMG2524-H	
MAC Address:	00:0D:DA:0D:52:FF	
System Up Time:	2 days 05:57:30	
iMG/RG Mgmt VLAN:	7	
Video VLAN:	40	
Internet Svc. VLAN:	20	
Voice VLAN:	10	
Internet Local VLAN:	2	
TLS VLAN (2..4094 or None):	None	
iMG/RG Additional VLAN IDs:	None	
Loop Detection:	Disabled	
SNTP Server (IP Addr. or None):	None	
Daylight Saving:	Enabled	
Time Zone:	EST	

	Current Value	New Value
iMG/RG General Profile :	None	
SysContact (Customer ID or None):	2524LANman	
SysLocation (location or None):	10.52.30.30_2.1	
SysName (system name or None):		
Limited User Login (login or None):	None	
New Limited User Password:	N/A	
New Manager Password:	N/A	
Super User Login (login or None):	None	
New Super User Password:	N/A	
DHCP Client Options:	3,121	

Current Mgmt. Subnets

Name	Subnet Addr.	Mask

New Mgmt. Subnets

Name	Subnet Addr.	Mask

Wed Aug 13 16:57:55 EDT 2014 - Polling of RG_1407956541161 successful.

FIGURE 21-19 Service management screen for an iMG 1000 or iMG 2000 device

21.14.2 Multi-service VLANs

Note the following when provisioning a multi-service VLAN configuration:

- If the internet service is Routed NAT and on the same VLAN as the RG Mgmt VLAN, you must have the Firewall=ON and two port filters to allow TCP and ICMP traffic. Otherwise the NMS will lose connectivity and cannot discover the iMG.
- When moving a service from one shared VLAN to another VLAN, the LAN ports move with the service, so a port for a service for video may, for example, end up with a port as Internet. In the port assignment tab of the RG General Form, the user must look at the configuration and decide which port will have the video. Refer to Configuring multi-service VLAN.
- If you are adding internet service to a working VLAN (which already has DHCP and IP addresses), note the following:
- If in the internet profile there is a mismatch, you will get an error message.
- Once the internet service is joined, you can change the DHCP settings.
- If taking internet service out of a shared service VLAN, internet service could be lost. Refer to Configuring multi-service VLAN
- TLS service must always have its own VLAN.
- The local RG VLAN is separate.

- Prior to release 10.0, if Bridged Internet service was configured, the DHCP and IP address/mask fields were grayed out, now they are not, since you may want to add another service such as voice.

21.14.3 iMG6x6MOD/iMG7x6MOD - Translation and HPNA Diagnostics

21.14.3.1 Need for Translation of VLAN Numbering for iMG6x6MOD

With the iMG6x6MOD product, the media converter used between the coax and ethernet interfaces has untagged VLANs on the ethernet interfaces, numbered 201 and 901. The VLANs used on the LAN ports must also have these two VIDs configured.

Note: The HPNA could also be configured to support an untagged VLAN, but this needs to be configured on the default VLAN (1), and the HPNA could support only one service.

Since the upstream network might not be using VLANs 201 and 901 as their VLANs for data and video, the VLAN must be translated to another VID that matches what the network is using. Using this translation feature for iMAP interfaces is available on the Port Profile Form.

21.14.3.2 HPNA Testing Feature

The HPNA card allows the end-user to use the existing Coax cables in the home as part of the home network. One of the problems with this model is the varying quality of the Coax cable and connectors. To help the service provider diagnose problems inside the home, the iMG6x6MOD/iMG7x6MOD provides data on the HPNA network. This feature allows the service provider use the NMS to diagnose problems in their customer's HPNA network.

The feature allows the user to perform the following:

- View the information about the master station (iMG) of the HPNA Network.
- View the information about each of the stations in the HPNA network. This includes the list of hosts (MAC Addrs) behind each of the stations.
- View the HPNA statistics for each of the stations in the HPNA network.
- Reset the HPNA statistics for the stations in the HPNA network.
- Request the collection of the HPNA network performance metrics and view the result of the test.
- When requesting the collection of HPNA network performance metrics, the user is warned that this request is service affecting. In addition, user can cancel the request upon seeing the warning before the service is affected.

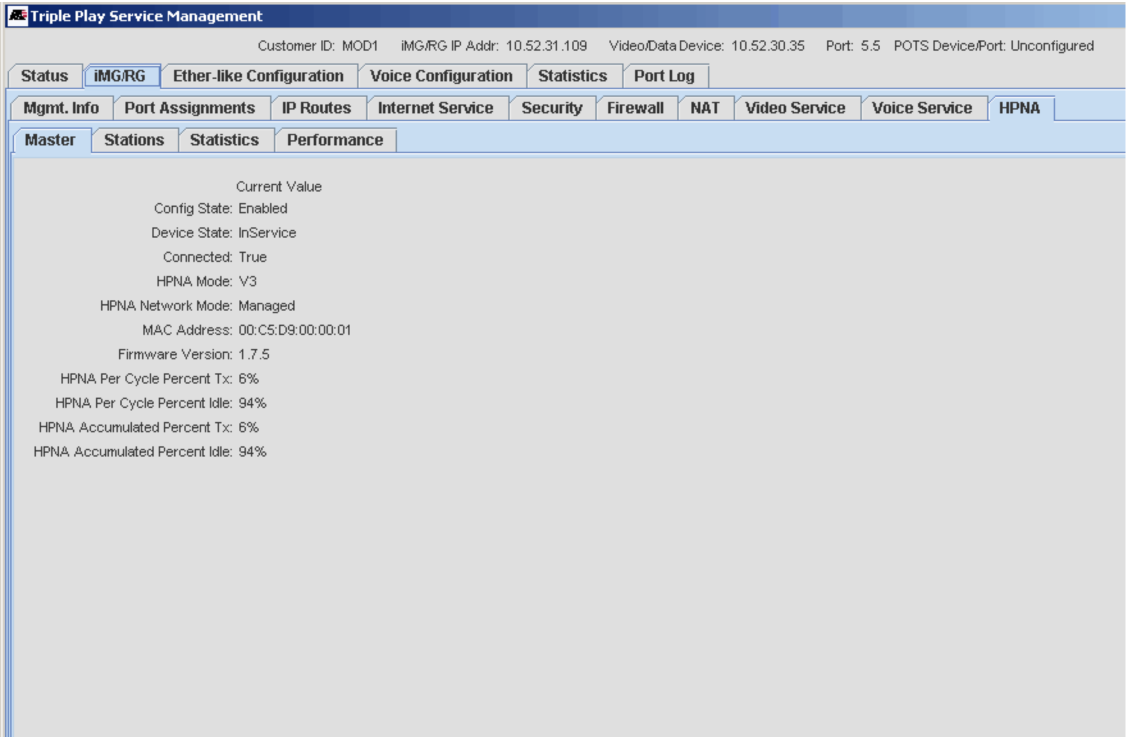
Note: The performance metrics collection will not be polled. The user must specifically request the metrics collection to be taken.

This feature consists of using four tabs:

1. HPNA network master information - The user can access this tab as follows:

- The iMG/RG Network Inventory or the IP Network Map, the user can select an iMG6x6MOD/iMG7x6MOD and select the “View/Modify Details” button.
- From the Triple Management window that is brought up, the user can select the “iMG/RG” tab. This will bring up the General information about the iMG. The user then selects the HPNA sub-tab. This will display the Master Tab containing the information on the master of the HPNA Network.

Refer to the following figure



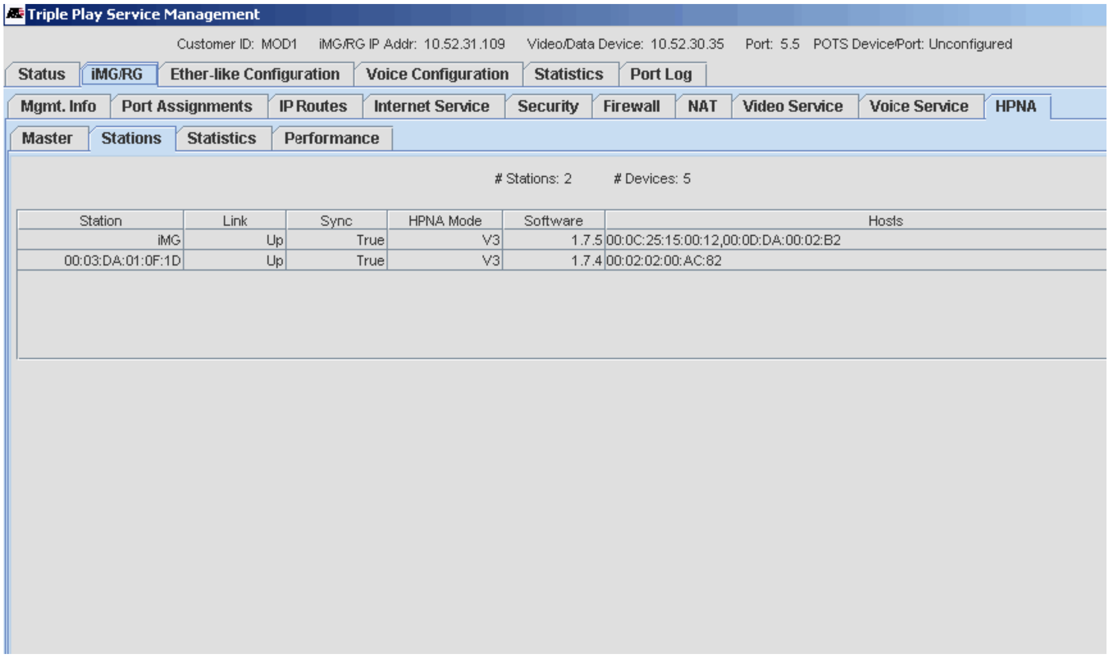
Customer ID: MOD1 iMG/RG IP Addr: 10.52.31.109 Video/Data Device: 10.52.30.35 Port: 5.5 POTS Device/Port: Unconfigured

	Current Value
Config State:	Enabled
Device State:	InService
Connected:	True
HPNA Mode:	V3
HPNA Network Mode:	Managed
MAC Address:	00:C5:D9:00:00:01
Firmware Version:	1.7.5
HPNA Per Cycle Percent Tx:	6%
HPNA Per Cycle Percent Idle:	94%
HPNA Accumulated Percent Tx:	6%
HPNA Accumulated Percent Idle:	94%

FIGURE 21-20 HPNA Testing - Master Tab

2. View the HPNA network stations information - The user can view the information about the stations in the HPNA network. The information to be displayed is shown in the diagram.

   The Stations sub-tab contains the HPNA Network station information. The tab will show a table where each row contains information on a different station including the Station MAC Address, the Link State, the Sync State, the HPNA Mode, the software level, and a list of the hosts attached to that station. Refer to the following figure.



Customer ID: MOD1 iMG/RG IP Addr: 10.52.31.109 Video/Data Device: 10.52.30.35 Port: 5.5 POTS Device/Port: Unconfigured

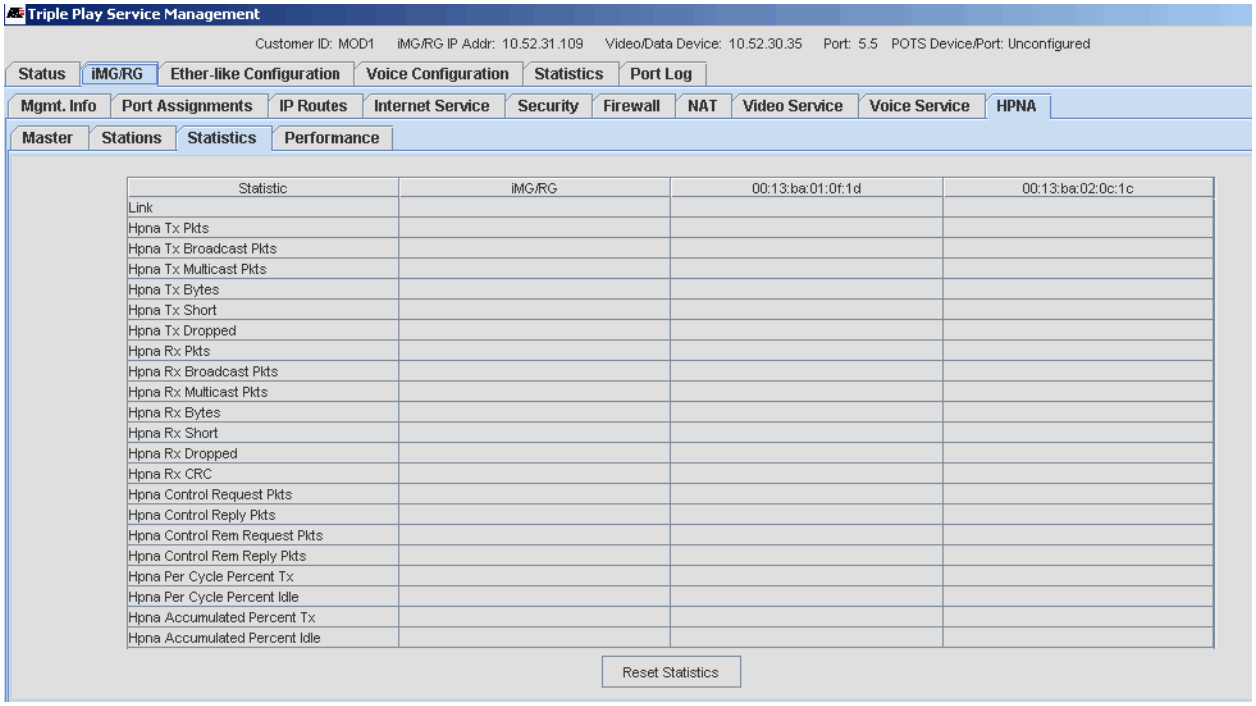
Stations: 2 # Devices: 5

Station	Link	Sync	HPNA Mode	Software	Hosts
iMG	Up	True	V3	1.7.5	00:0C:25:15:00:12,00:0D:DA:00:02:B2
00:03:DA:01:0F:1D	Up	True	V3	1.7.4	00:02:02:00:AC:82

FIGURE 21-21 HPNA Testing - Stations Tab

3. View the HPNA network statistics - The user can view the statistics for each of the stations in the HPNA network.

   The Statistics Tab contains the HPNA Network station statistics. The tab will show a table where each row is a different statistic and each column is a station in the HPNA Network. The user can press the “Reset Statistics” button, and the HPNA statistics on the iMG are set back to 0. Refer to the following figure.



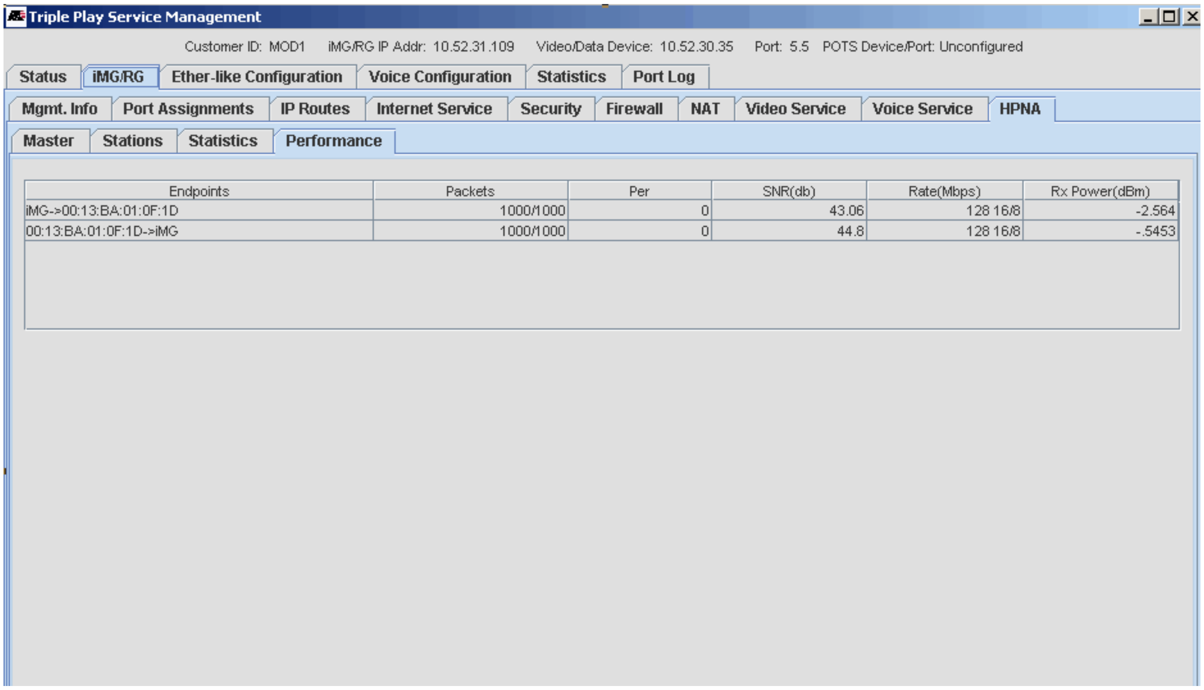
Customer ID: MOD1 iMG/RG IP Addr: 10.52.31.109 Video/Data Device: 10.52.30.35 Port: 5.5 POTS Device/Port: Unconfigured

Statistic	iMG/RG	00:13:ba:01:0f:1d	00:13:ba:02:0c:1c
Link			
Hpna Tx Pkts			
Hpna Tx Broadcast Pkts			
Hpna Tx Multicast Pkts			
Hpna Tx Bytes			
Hpna Tx Short			
Hpna Tx Dropped			
Hpna Rx Pkts			
Hpna Rx Broadcast Pkts			
Hpna Rx Multicast Pkts			
Hpna Rx Bytes			
Hpna Rx Short			
Hpna Rx Dropped			
Hpna Rx CRC			
Hpna Control Request Pkts			
Hpna Control Reply Pkts			
Hpna Control Rem Request Pkts			
Hpna Control Rem Reply Pkts			
Hpna Per Cycle Percent Tx			
Hpna Per Cycle Percent Idle			
Hpna Accumulated Percent Tx			
Hpna Accumulated Percent Idle			

FIGURE 21-22 HPNA Testing - Statistics Tab

4. View the HPNA performance metrics

The user can view the performance metrics between each pair of stations in the HPNA network. The tab will show a table where each row is a different from-station/to-station pair and each column is a metric. The user then presses the “Collect Performance Metrics” buttons to start the data collection. Refer to the following figure.



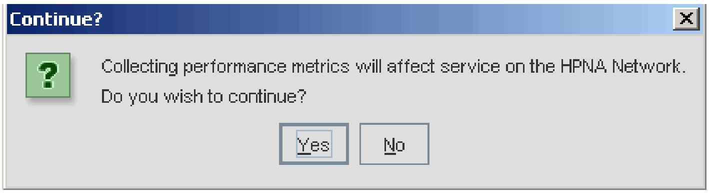
Customer ID: MOD1 iMG/RG IP Addr: 10.52.31.109 Video/Data Device: 10.52.30.35 Port: 5.5 POTS Device/Port: Unconfigured

Endpoints	Packets	Per	SNR(db)	Rate(Mbps)	Rx Power(dBm)
iMG->00:13:BA:01:0F:1D	1000/1000	0	43.06	128 16/8	-2.564
00:13:BA:01:0F:1D->iMG	1000/1000	0	44.8	128 16/8	-.5453

FIGURE 21-23 HPNA - Performance Tab

5. Collect Performance Metrics

The user selects the Performance sub-tab and presses the “Collect Performance Metrics” button. This will display confirmation dialog as shown in the following figure.



Collecting performance metrics will affect service on the HPNA Network.
Do you wish to continue?

FIGURE 21-24 HPNA Testing - Confirmation Window since will affect Service

6.The user then presses the No button to cancel the operation before service is affected.

21.14.4 iBG915-FX

With the iBG915-FX, the main difference between this CPE and CPE already supported is that the iBG915-FX supports 8 VoIP lines, four more than any previous iMG/RGs. Also, the iBG915-FX supports 5 LAN ports, rather than 3, 4 or 6 LAN ports.

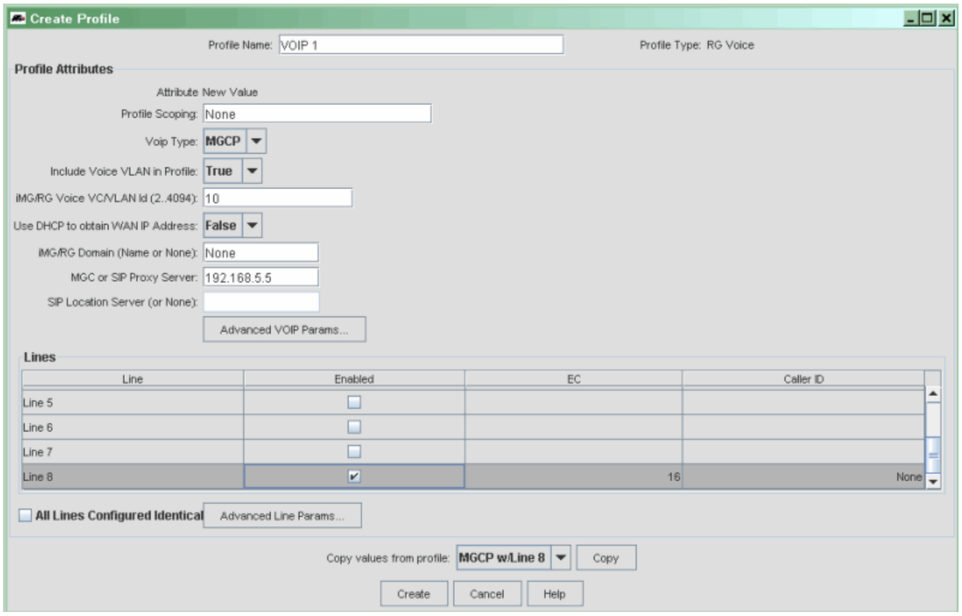
The NMS provides the same support as other iMG/RGs (discovery support, triple play provisioning/de-provisioning and management support, iMG/RG profile support, GenBand interworking support, backup/restore support, software download support, and “Device Info” support.

Note: CPU-based rate limiting is supported, as with the iMG MOD devices. This feature is included in the following subsections.

21.14.4.1 Changes to the GUI

- iMG/RG Voice Profile Windows

  The iMG/RG Voice Profile screen is modified to allow the user to specify the configuration to be applied to lines 5 through 8. Refer to the following figures.



Profile Name: VOIP 1

Profile Type: RG Voice

Profile Attributes

Attribute New Value

Profile Scoping: None

Voip Type: MGCP

Include Voice VLAN in Profile: True

iMG/RG Voice VC/VLAN Id (2..4094): 10

Use DHCP to obtain WAN IP Address: False

iMG/RG Domain (Name or None): None

MGC or SIP Proxy Server: 192.168.5.5

SIP Location Server (or None):

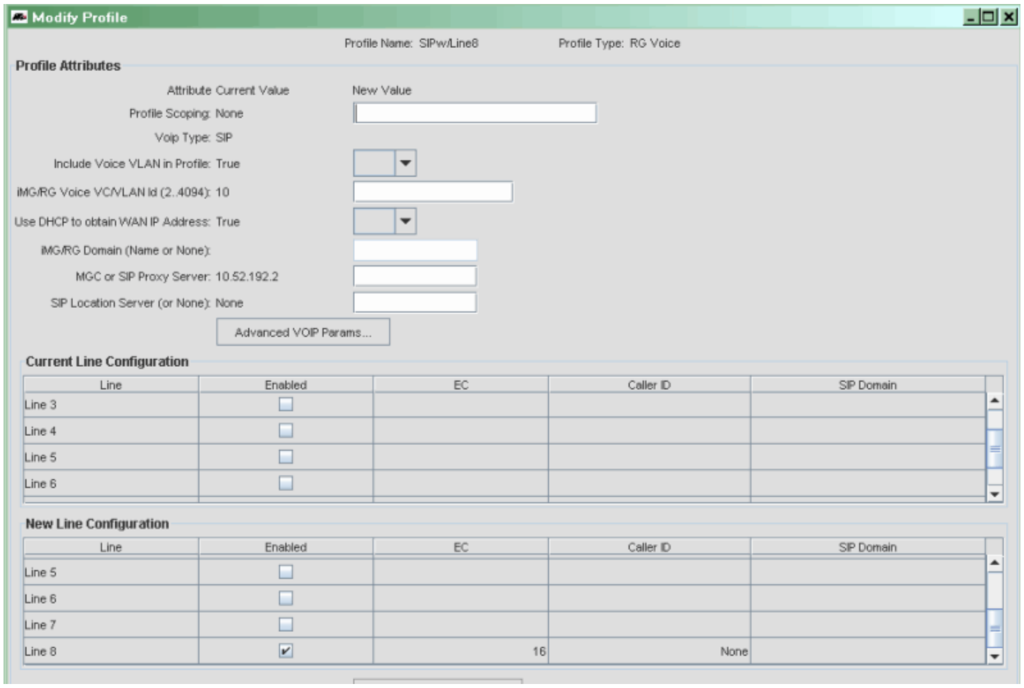
Lines

Line	Enabled	EC	Caller ID
Line 5	□		
Line 6	□		
Line 7	□		
Line 8	☑	16	None

□ All Lines Configured Identical

Copy values from profile: MGCP w/Line 8

FIGURE 21-25 Voice Profile for iBG915-FX



Profile Name: SIPw/Line8

Profile Type: RG Voice

Profile Attributes

Attribute	Current Value	New Value
Profile Scoping:	None	
Voip Type:	SIP	
Include Voice VLAN in Profile:	True	
iMG/RG Voice VC/VLAN Id (2..4094):	10	
Use DHCP to obtain WAN IP Address:	True	
iMG/RG Domain (Name or None):		
MGC or SIP Proxy Server:	10.52.192.2	
SIP Location Server (or None):	None	

Current Line Configuration

Line	Enabled	EC	Caller ID	SIP Domain
Line 3	□			
Line 4	□			
Line 5	□			
Line 6	□			

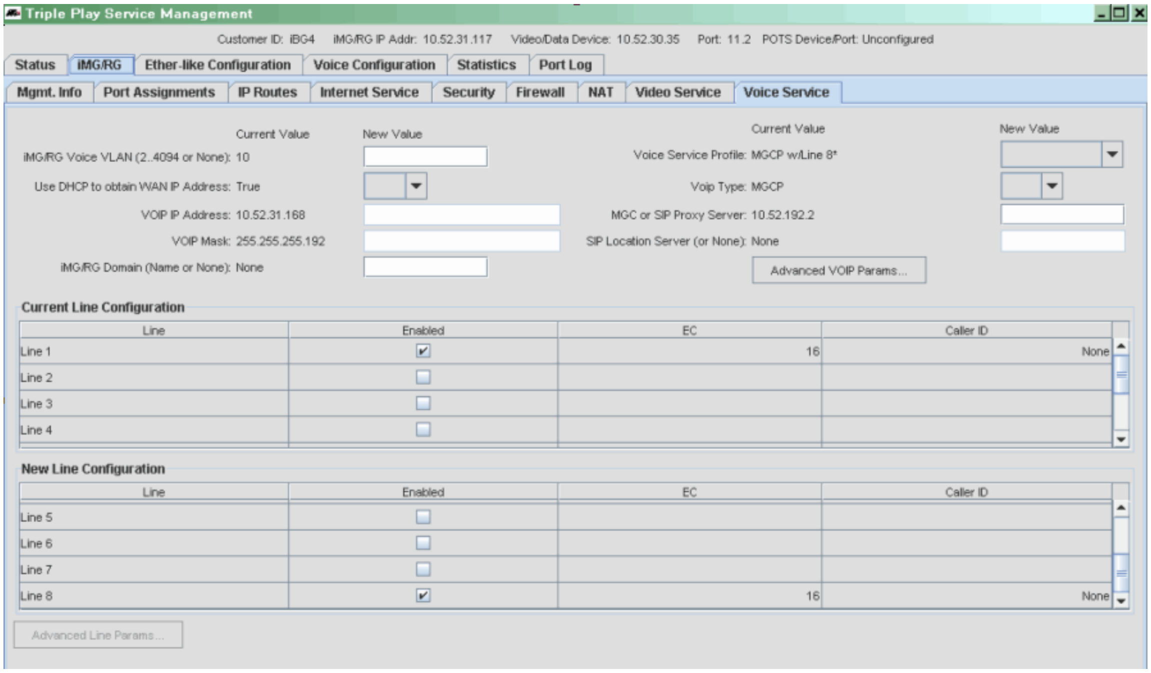
New Line Configuration

Line	Enabled	EC	Caller ID	SIP Domain
Line 5	□			
Line 6	□			
Line 7	□			
Line 8	☑	16	None	

FIGURE 21-26 Modify iMG/RG Voice Profile for iBG915-FX

- iMG/RG Voice Service Tab on the Triple Play Service Management Window

The iMG/RG Voice Service Tab of the Triple Play Service Management window is updated to show the current configuration of all eight voice lines on the iBG915-FX.   In addition, the user can make updates to those additional lines. Refer to the following figure.



Customer ID: iBG4 iMG/RG IP Addr: 10.52.31.117 Video/Data Device: 10.52.30.35 Port: 11.2 POTS Device/Port: Unconfigured

	Current Value	New Value
iMG/RG Voice VLAN (2..4094 or None):	10	
Use DHCP to obtain WAN IP Address:	True	
VOIP IP Address:	10.52.31.168	
VOIP Mask:	255.255.255.192	
iMG/RG Domain (Name or None):	None	

	Current Value	New Value
Voice Service Profile:	MGCP w/Line 8*	
Voip Type:	MGCP	
MGC or SIP Proxy Server:	10.52.192.2	
SIP Location Server (or None):	None	

Current Line Configuration

Line	Enabled	EC	Caller ID
Line 1	☑	16	None
Line 2	☐		
Line 3	☐		
Line 4	☐		

New Line Configuration

Line	Enabled	EC	Caller ID
Line 5	☐		
Line 6	☐		
Line 7	☐		
Line 8	☑	16	None

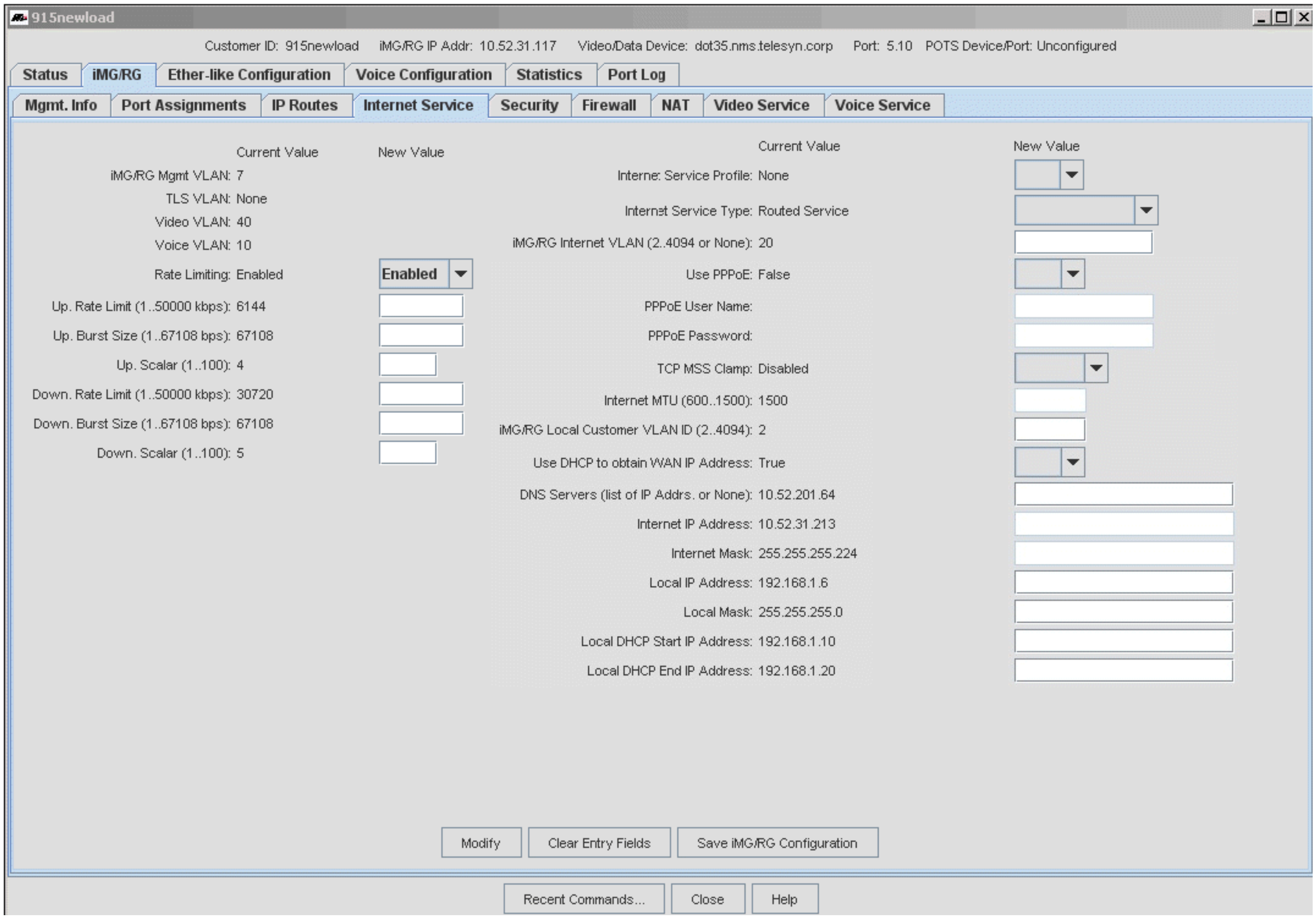
FIGURE 21-27 Service Management for iBG915-FX

- iMG/RG General Tab on the Triple Play Service Management Window

  The iMG/RG General Tab of the Triple Play Service Management window is updated to **not** display the RG Loopback detection field when viewing an iBG915-FX.

- iMG/RG Internet Service Tab on the Triple Play Service Management Window

  The iMG/RG Service Tab of the Triple Play Service Management window shows the Service Rate Limiting fields. (PPPoE continues not to be shown.). Refer to the following figure.



Customer ID: 915newload iMG/RG IP Addr: 10.52.31.117 Video/Data Device: dot35.nms.telesyn.corp Port: 5.10 POTS Device/Port: Unconfigured

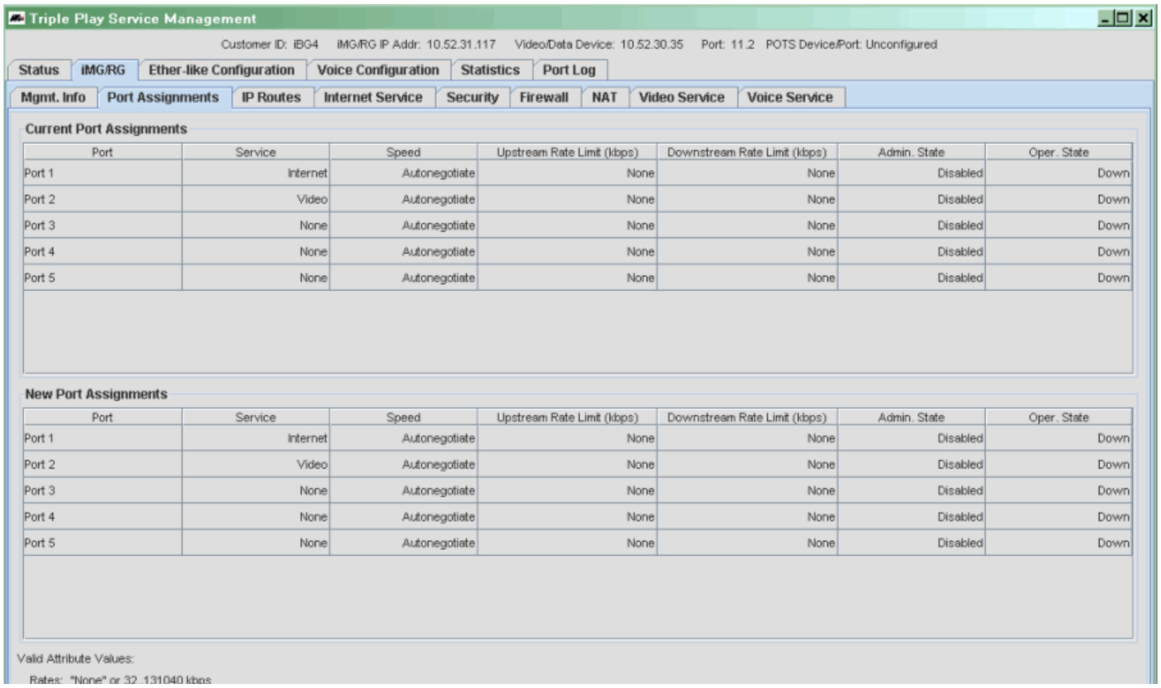
	Current Value	New Value
iMG/RG Mgmt VLAN:	7	
TLS VLAN:	None	
Video VLAN:	40	
Voice VLAN:	10	
Rate Limiting:	Enabled	Enabled
Up. Rate Limit (1..50000 kbps):	6144	
Up. Burst Size (1..67108 bps):	67108	
Up. Scalar (1..100):	4	
Down. Rate Limit (1..50000 kbps):	30720	
Down. Burst Size (1..67108 bps):	67108	
Down. Scalar (1..100):	5	

	Current Value	New Value
Interne: Service Profile:	None	
Internet Service Type:	Routed Service	
iMG/RG Internet VLAN (2..4094 or None):	20	
Use PPPoE:	False	
PPPoE User Name:		
PPPoE Password:		
TCP MSS Clamp:	Disabled	
Internet MTU (600..1500):	1500	
iMG/RG Local Customer VLAN ID (2..4094):	2	
Use DHCP to obtain WAN IP Address:	True	
DNS Servers (list of IP Addrs. or None):	10.52.201.64	
Internet IP Address:	10.52.31.213	
Internet Mask:	255.255.255.224	
Local IP Address:	192.168.1.6	
Local Mask:	255.255.255.0	
Local DHCP Start IP Address:	192.168.1.10	
Local DHCP End IP Address:	192.168.1.20	

FIGURE 21-28 iBG915-FX - Internet tab includes CPU-based Rate Limiting

- iMG/RG Port Assignment Tab on the Triple Play Service Management Window

  The iMG/RG Port Assignment Tab of the Triple Play Service Management window is updated to show the current configuration of the five LAN ports on the iBG915-FX. In addition, the user can make updates to those ports. Refer to the following figure.



Customer ID: iBG4 iMG/RG IP Addr: 10.52.31.117 Video/Data Device: 10.52.30.35 Port: 11.2 POTS Device/Port: Unconfigured

Current Port Assignments

Port	Service	Speed	Upstream Rate Limit (kbps)	Downstream Rate Limit (kbps)	Admin. State	Oper. State
Port 1	Internet	Autonegotiate	None	None	Disabled	Down
Port 2	Video	Autonegotiate	None	None	Disabled	Down
Port 3	None	Autonegotiate	None	None	Disabled	Down
Port 4	None	Autonegotiate	None	None	Disabled	Down
Port 5	None	Autonegotiate	None	None	Disabled	Down

New Port Assignments

Port	Service	Speed	Upstream Rate Limit (kbps)	Downstream Rate Limit (kbps)	Admin. State	Oper. State
Port 1	Internet	Autonegotiate	None	None	Disabled	Down
Port 2	Video	Autonegotiate	None	None	Disabled	Down
Port 3	None	Autonegotiate	None	None	Disabled	Down
Port 4	None	Autonegotiate	None	None	Disabled	Down
Port 5	None	Autonegotiate	None	None	Disabled	Down

Valid Attribute Values:

Rates: "None" or 32..131040 kbps

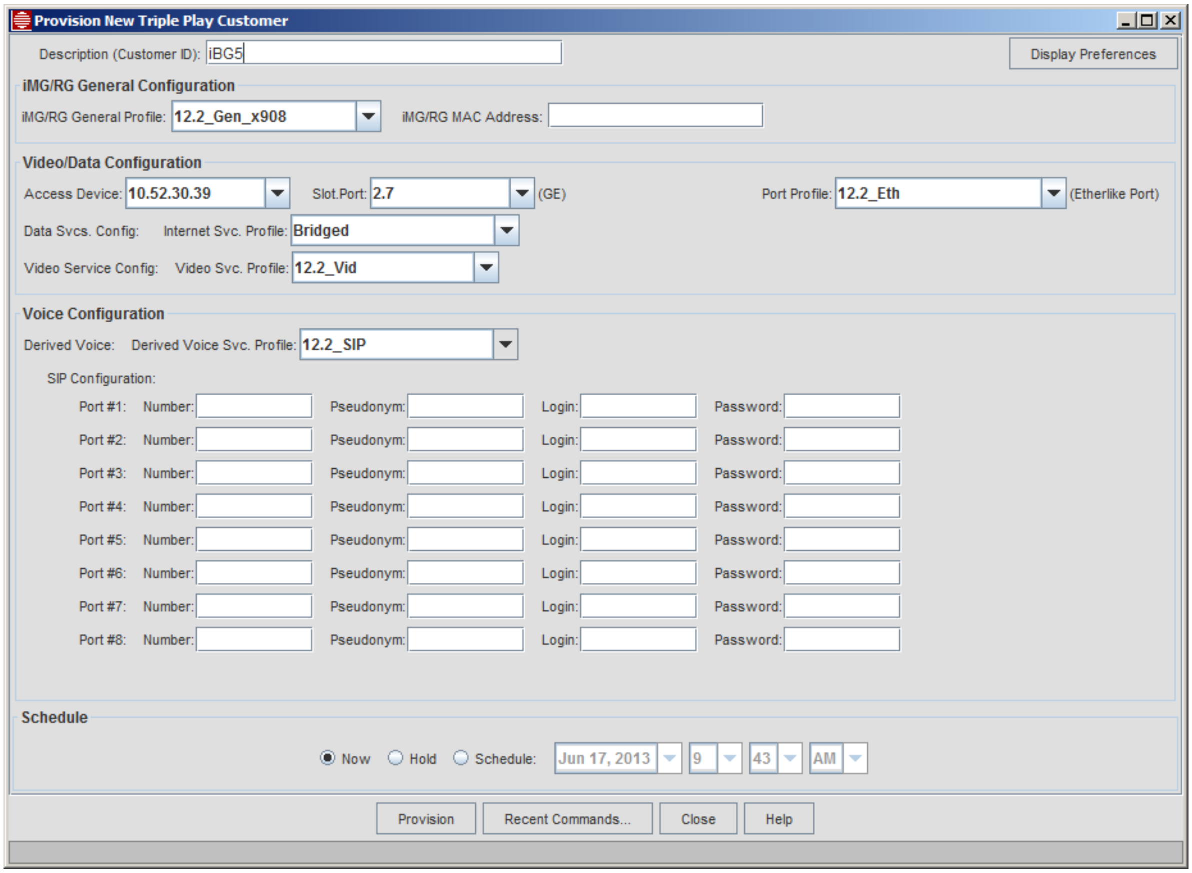
FIGURE 21-29 iBG915-FX Port Assignments

- iMG/RG Video Tab on the Triple Play Service Management Window

  Like the iMG6x6-MOD CPEs, the iBG915-FX does not support the IGMP security feature present on some of the other iMG/RGs. Because of this, the IGMP Security, IGMP Security Autolearning, and Trusted Host Limit fields, along with the Locked STD MAC Addresses table are **not** displayed on the Video Tab.

- Provision New Triple Play Customer Window

  The Provision New Triple Play Customer Window is updated to allow the user to enter the configuration of up to eight voice lines (depending on the number of voice line configured in the selected iMG/RG voice profile). Refer to the following figure.



Provision New Triple Play Customer

Description (Customer ID): iBG5

iMG/RG General Configuration

iMG/RG General Profile: 12.2_Gen_x908

iMG/RG MAC Address:

Video/Data Configuration

Access Device: 10.52.30.39

Slot.Port: 2.7 (GE)

Port Profile: 12.2_Eth (Etherlike Port)

Data Svcs. Config: Internet Svc. Profile: Bridged

Video Service Config: Video Svc. Profile: 12.2_Vid

Voice Configuration

Derived Voice: Derived Voice Svc. Profile: 12.2_SIP

SIP Configuration:

Port #1:	Number:	Pseudonym:	Login:	Password:
Port #2:	Number:	Pseudonym:	Login:	Password:
Port #3:	Number:	Pseudonym:	Login:	Password:
Port #4:	Number:	Pseudonym:	Login:	Password:
Port #5:	Number:	Pseudonym:	Login:	Password:
Port #6:	Number:	Pseudonym:	Login:	Password:
Port #7:	Number:	Pseudonym:	Login:	Password:
Port #8:	Number:	Pseudonym:	Login:	Password:

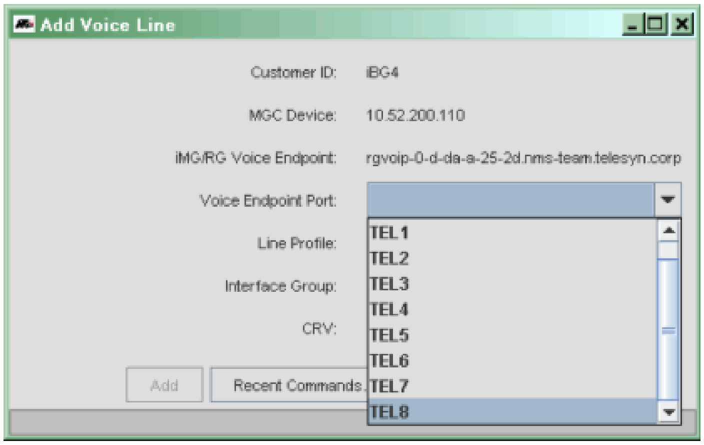
Schedule

● Now ○ Hold ○ Schedule: Jun 17, 2013 9 43 AM

FIGURE 21-30 Provisioning New Customer for iBG915-FX

- GenBand G2/G6 - Add Voice Line Window

The window that allows that user to configure a voice line for an IBG915-FX on the GenBand G6 is modified to allow the user to specify telephone ports 5-8. Refer to the following figure.



Add Voice Line

Customer ID: iBG4

MGC Device: 10.52.200.110

iMG/RG Voice Endpoint: rgvoip-0-d-da-a-25-2d.nms-team.telesyn.corp

Voice Endpoint Port:

FIGURE 21-31 Adding a Voice Line to the iBG915-FX

21.14.5 iMG with WAN 1G Module

Products such as the AT-iMG7x6MOD can support the same card configuration as the AT-iMG6x6MOD, described in Configuration 7 - iMG7x6MOD with HPNA. In addition, it can support the following:

- 1 Gigabit Bidirectional WAN Module
- 1 Gigabit Bidirectional WAN Module with a Gigabit LANRJ-45 connection, allowing both the LAN and WAN ports to be configured on one module. (See notes)

Note: *When provisioning using the NMS, the user will configure the LAN connection on the WAN module as G-Lan.*

Note: *Inserting the WAN card with the copper LAN interface disables the interface to the DS1/T1 card, and so the DS1/E1 card cannot be used.*

Note: *When either of the 1 Gigabit WAN cards is configured, the connection to the iMAP can only be with certain GE interfaces, as follows.Refer to Provisioning Changes.*

Note: *To provision the iMG/RG off the GE interface and have DHCP forwarding work, the Etherlike port Profile now includes the field Direction (either Network or Customer), in which the Direction is set to Customer. Refer to Provisioning Changes.*

- Support of the HPNA 320 Module

The following figure shows a sample configuration. This is a simplified figure, since the VLAN configuration is the same as the iMG6x6MOD, as shown in Figure 24-27.

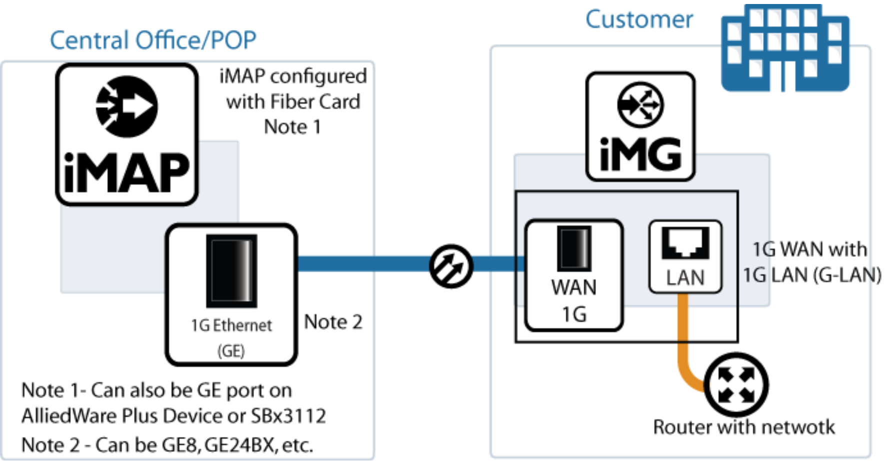

Central Office/POP
iMAP configured with Fiber Card Note 1
iMAP
1G Ethernet (GE)
Note 2
Note 1- Can also be GE port on AlliedWare Plus Device or SBx3112
Note 2 - Can be GE8, GE24BX, etc.
Customer
iMG
WAN 1G
LAN
1G WAN with 1G LAN (G-LAN)
Router with netwotk

FIGURE 21-32 Example iMG7x6MOD Configuration (Simplified)

21.14.5.1 Provisioning Changes

When the iMG (such as the iMG7x6MOD or iMG726BD-ON) is configured with a 1G WAN card, the associated iMAP card must support a direction of Customer, so the GE port **must** be configured with a direction of customer (rather than network.). To allow for this, there are the following changes in provisioning:

- The provisioning of a GE port brings up the Triple-Play provisioning to allow for the configuration of an iMG/RG on that port.
- Previously, a GE port was by default set to “Network”. To provision an iMG/RG off the port and have DHCP forwarding work, the Etherlike port Profile now includes the field Direction (either Network or Customer). Moreover, the default for this field is now Customer (rather than the implicit Network).

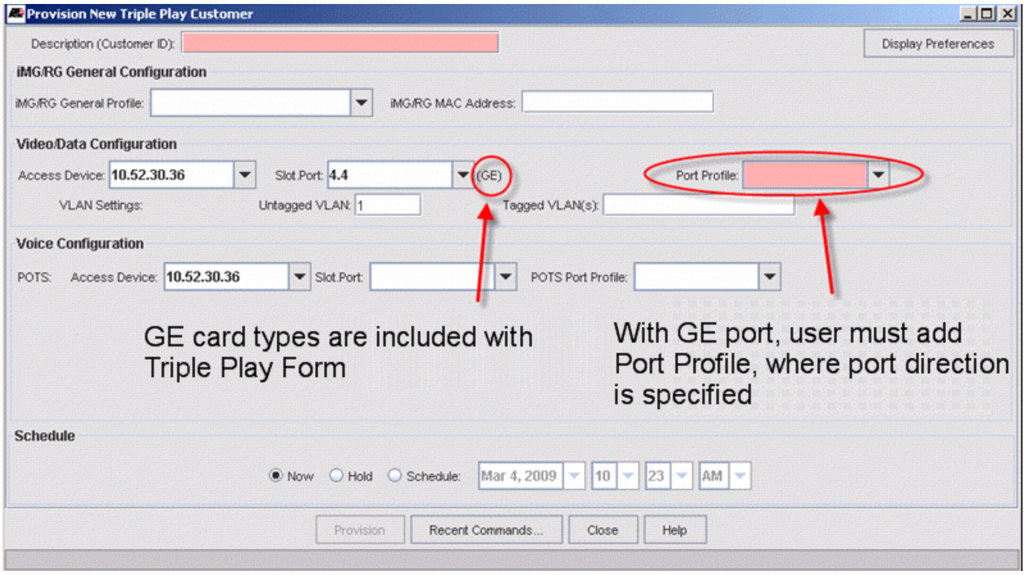
For existing Ethernet port profiles these changes are not an issue, because they will not have the port direction field explicitly set. However, **new port profiles should be created with the port direction set to match the provisioning scenario in which they will be used**, as follows:

The following iMAP GE ports should have new profiles set with the direction of Customer when connecting with with a 1G WAN card

- GE8 on the 9x00 iMAP
- GE4 (5.0-5.3) on the iMAP 910x
- GE24BX on 9000 series iMAP
- GE24SFP and GE40CSFP on SBx3100

Caution: *Modifying an existing ethernet port profile is possible but carries risks, since you will now set the port direction. Setting it to 'Customer' for an existing Ethernet port may stop service. Setting it to 'Network' on an FE/FX port with an iMG/RG (where the administrator could set the port direction to 'Customer' at the CLI) will cause the DHCP to no longer function.*

Refer to the following figures.



Provision New Triple Play Customer

Description (Customer ID):

iMG/RG General Configuration

iMG/RG General Profile:

iMG/RG MAC Address:

Video/Data Configuration

Access Device: 10.52.30.36

Slot.Port: 4.4 (GE)

Port Profile:

VLAN Settings:

Untagged VLAN: 1

Tagged VLAN(s):

Voice Configuration

POTS: Access Device: 10.52.30.36

Slot.Port:

POTS Port Profile:

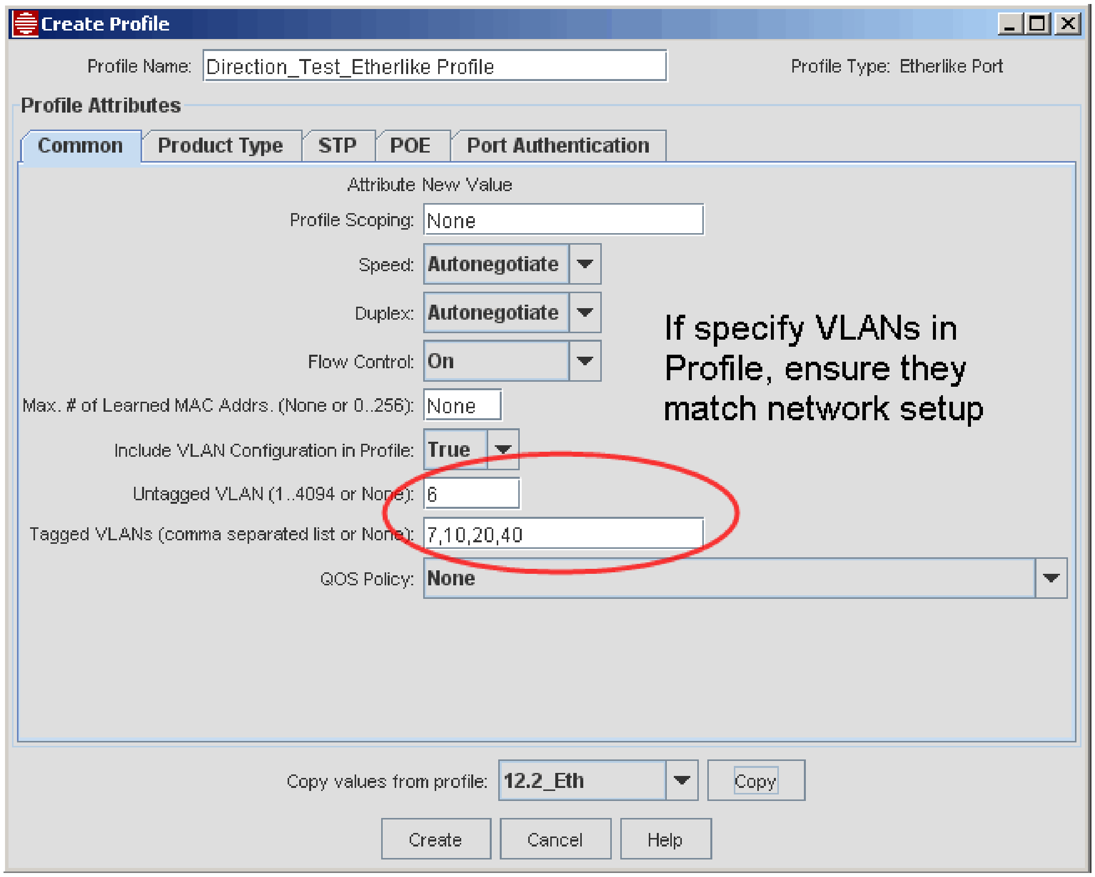
GE card types are included with Triple Play Form

With GE port, user must add Port Profile, where port direction is specified

Schedule

● Now ○ Hold ○ Schedule: Mar 4, 2009 10 23 AM

FIGURE 21-33 Provision New Triple Play Form for GE8/GE24BX/AW+/GE24SFP Port



Profile Name: Direction_Test_Etherlike Profile

Profile Type: Etherlike Port

Profile Attributes

Attribute New Value

Profile Scoping: None

Speed: Autonegotiate

Duplex: Autonegotiate

Flow Control: On

Max. # of Learned MAC Addrs. (None or 0..256): None

Include VLAN Configuration in Profile: True

Untagged VLAN (1..4094 or None): 6

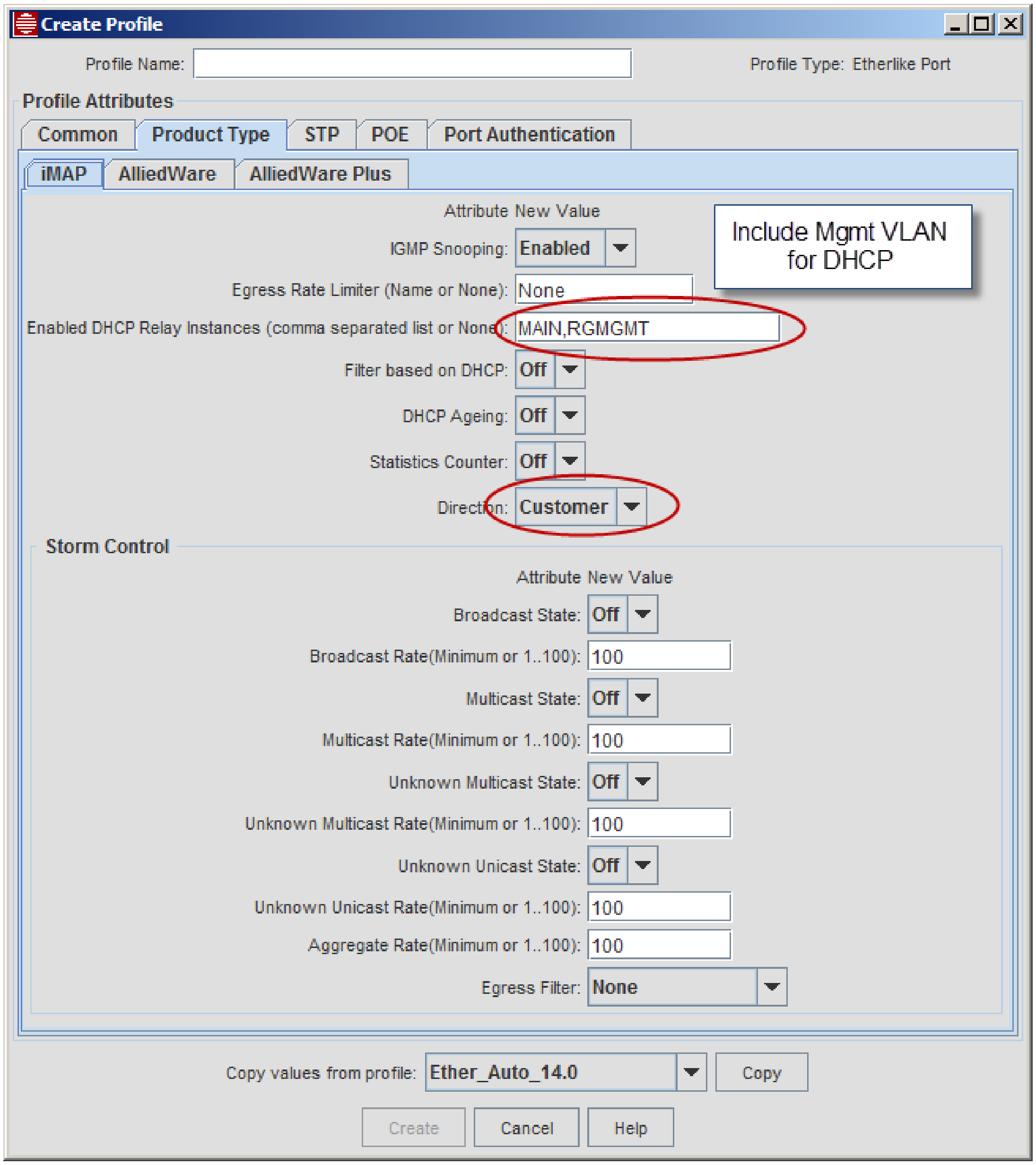
Tagged VLANs (comma separated list or None): 7,10,20,40

QOS Policy: None

Copy values from profile: 12.2_Eth

If specify VLANs in Profile, ensure they match network setup

FIGURE 21-34 Setting the GE Port profile to Provision the VLANs



Profile Name:

Profile Type: Etherlike Port

Profile Attributes

Attribute New Value

IGMP Snooping: Enabled

Egress Rate Limiter (Name or None): None

Enabled DHCP Relay Instances (comma separated list or None): MAIN,RGMGMT

Filter based on DHCP: Off

DHCP Ageing: Off

Statistics Counter: Off

Direction: Customer

Include Mgmt VLAN for DHCP

Storm Control

Attribute New Value

Broadcast State: Off

Broadcast Rate(Minimum or 1..100): 100

Multicast State: Off

Multicast Rate(Minimum or 1..100): 100

Unknown Multicast State: Off

Unknown Multicast Rate(Minimum or 1..100): 100

Unknown Unicast State: Off

Unknown Unicast Rate(Minimum or 1..100): 100

Aggregate Rate(Minimum or 1..100): 100

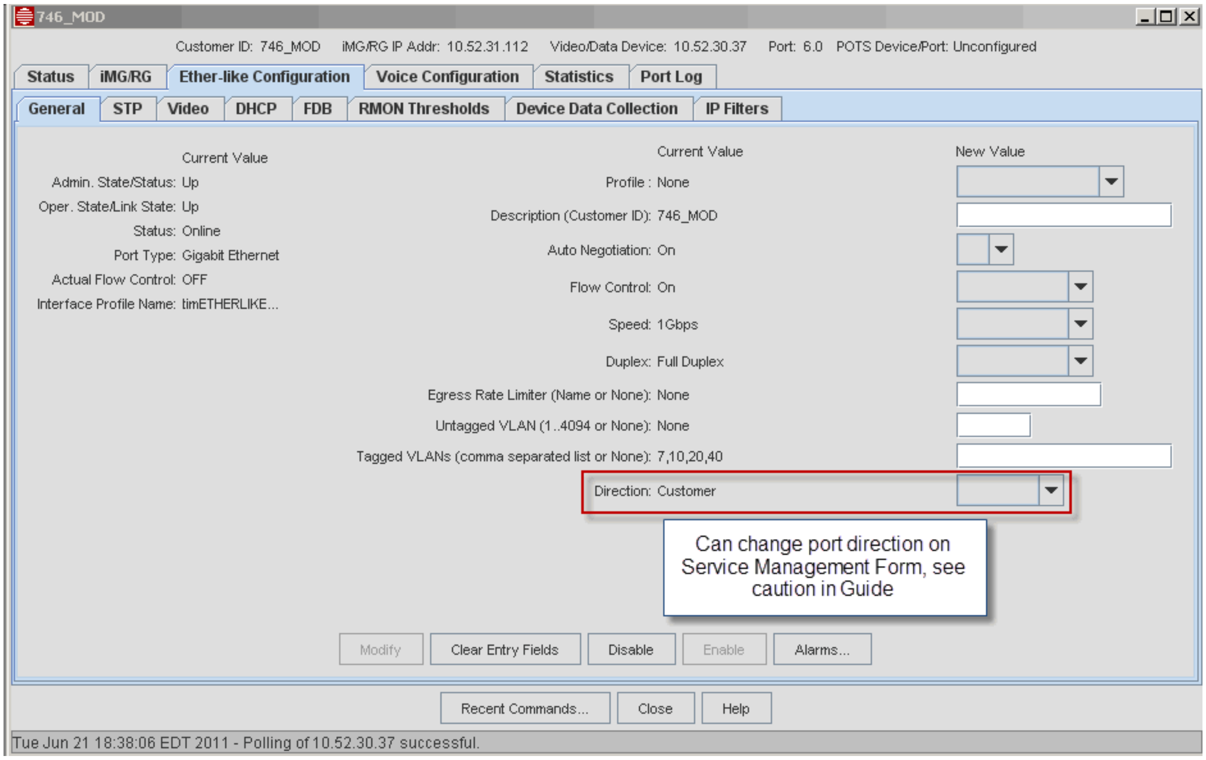
Egress Filter: None

Copy values from profile: Ether_Auto_14.0

FIGURE 21-35 Setting the GE Port profile to set Port Direction

As with other profile settings, the port direction can be (re)set on the Customer Management Form, under the Ether-like Configuration tab. Refer to the following figure.

Caution: *With the iMG7x6MOD, do not change the port direction once it has been set for Customer. To change the direction will mean a loss of service.*



Customer ID: 746_MOD iMG/RG IP Addr: 10.52.31.112 Video/Data Device: 10.52.30.37 Port: 6.0 POTS Device/Port: Unconfigured

Current Value

Admin. State/Status: Up
Oper. State/Link State: Up
Status: Online
Port Type: Gigabit Ethernet
Actual Flow Control: OFF
Interface Profile Name: timETHERLIKE...

Current Value / New Value

Profile : None
Description (Customer ID): 746_MOD
Auto Negotiation: On
Flow Control: On
Speed: 1Gbps
Duplex: Full Duplex
Egress Rate Limiter (Name or None): None
Untagged VLAN (1..4094 or None): None
Tagged VLANs (comma separated list or None): 7,10,20,40
Direction: Customer

Can change port direction on Service Management Form, see caution in Guide

Tue Jun 21 18:38:06 EDT 2011 - Polling of 10.52.30.37 successful.

FIGURE 21-36 Customer Management, showing Port Direction

The RG General profile includes the G-Lan ports (the ports available when the 1 Gigabit WAN with RJ-45 LAN card is used). When this card is used, the General profile includes the altered Port Assignments to allow the customer to provision services on the G-Lan ports.

21.14.6 Split Management for Wireless iMGs

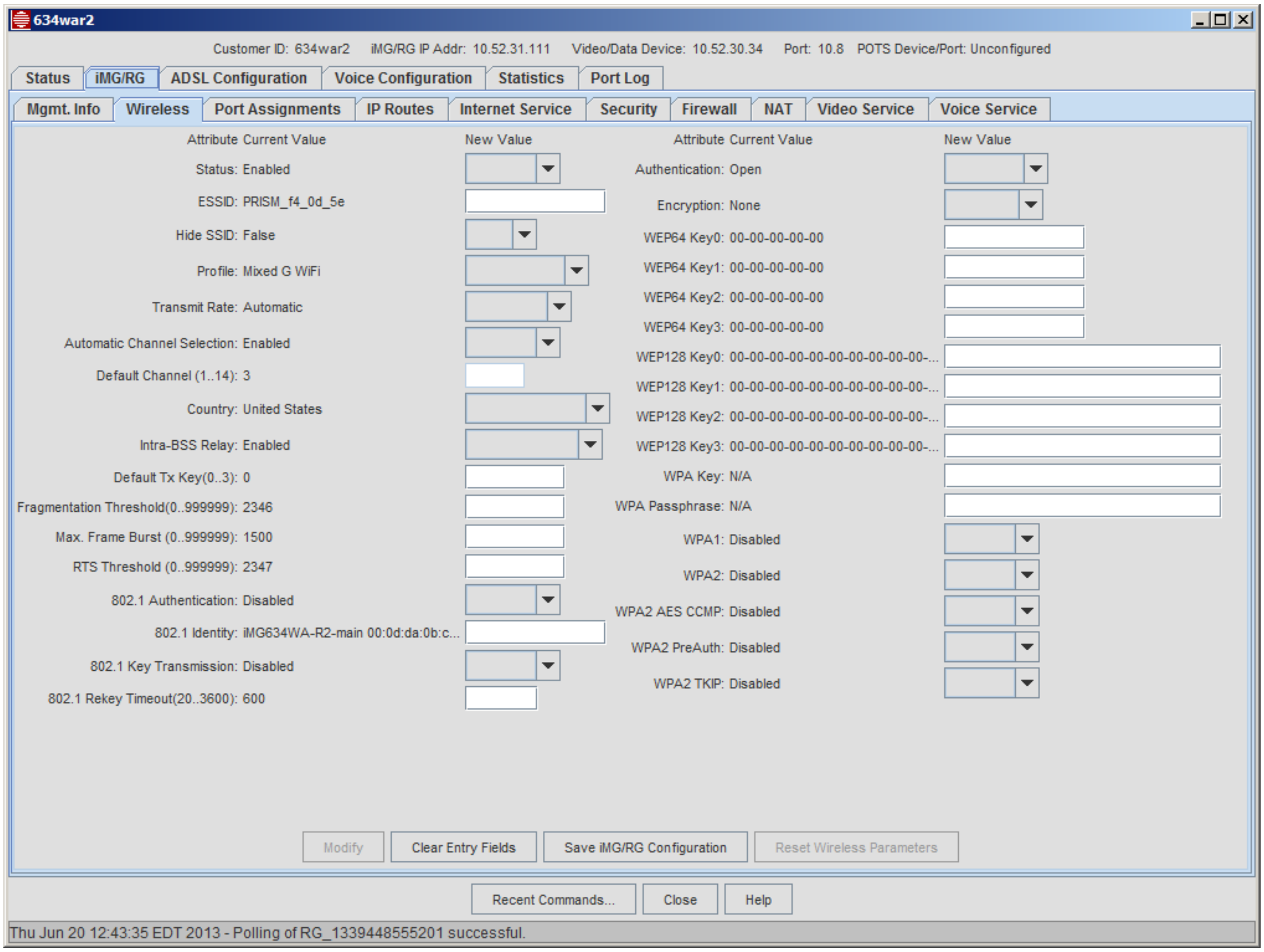
Split management allows subscribers to configure wireless parameters themselves through an iMG's administration web interface. Once you enable split management, subscribers can access the web interface and configure wireless parameters for the device.

Note: To access an iMG's administration web interface from within the NMS, in the iMG/RGs screen, right-click on the device and select Browse Device.

The following devices support split management:

- iMG634WA/B, running software release 3-7-04 or higher
- iMG634WA/B-R2, running software release 3-7-04 or higher
- iMG616W, running software release 3-7-04 or higher
- iMG 1000 and iMG 2000 series wireless devices, running software release 4.3 or higher

For iMG634WA/B, iMG634WA/B-R2 and iMG616W devices, when split management is enabled you cannot configure a device's wireless parameters through the NMS, it must be done through the iMG's administration web interface. When split management is disabled you can configure wireless parameters through the iMG/RG General profile, Wireless tab, or on an individual device through the iMG/RG - Wireless tab on the device's Service Management form:



Customer ID: 634war2 iMG/RG IP Addr: 10.52.31.111 Video/Data Device: 10.52.30.34 Port: 10.8 POTS Device/Port: Unconfigured

Status: Enabled
ESSID: PRISM_f4_0d_5e
Hide SSID: False
Profile: Mixed G WiFi
Transmit Rate: Automatic
Automatic Channel Selection: Enabled
Default Channel (1..14): 3
Country: United States
Intra-BSS Relay: Enabled
Default Tx Key(0..3): 0
Fragmentation Threshold(0..999999): 2346
Max. Frame Burst (0..999999): 1500
RTS Threshold (0..999999): 2347
802.1 Authentication: Disabled
802.1 Identity: iMG634WA-R2-main 00:0d:da:0b:c...
802.1 Key Transmission: Disabled
802.1 Rekey Timeout(20..3600): 600

Authentication: Open
Encryption: None
WEP64 Key0: 00-00-00-00-00
WEP64 Key1: 00-00-00-00-00
WEP64 Key2: 00-00-00-00-00
WEP64 Key3: 00-00-00-00-00
WEP128 Key0: 00-00-00-00-00-00-00-00-00-00-...
WEP128 Key1: 00-00-00-00-00-00-00-00-00-00-...
WEP128 Key2: 00-00-00-00-00-00-00-00-00-00-...
WEP128 Key3: 00-00-00-00-00-00-00-00-00-00-...
WPA Key: N/A
WPA Passphrase: N/A
WPA1: Disabled
WPA2: Disabled
WPA2 AES CCMP: Disabled
WPA2 PreAuth: Disabled
WPA2 TKIP: Disabled

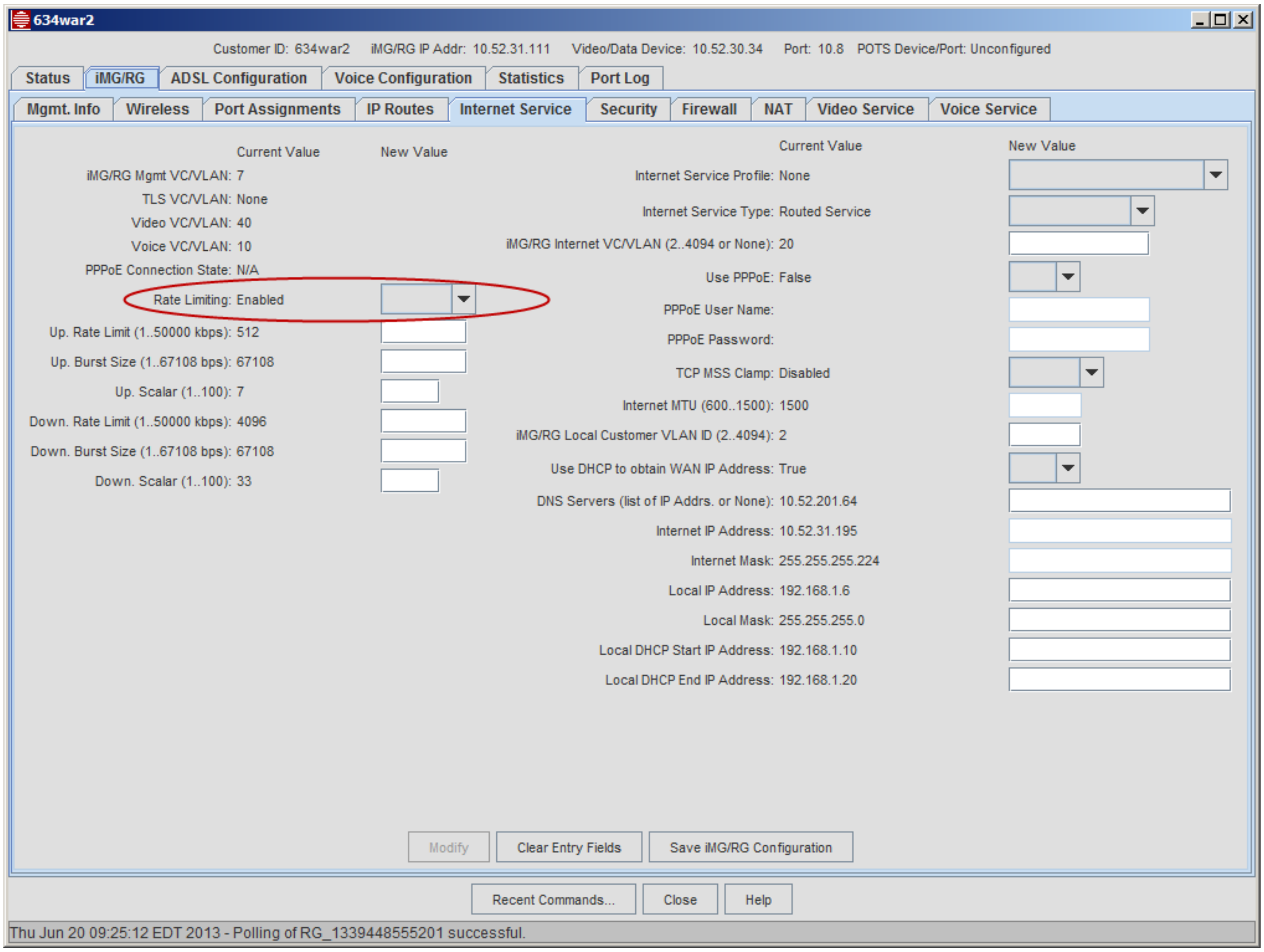
Thu Jun 20 12:43:35 EDT 2013 - Polling of RG_1339448555201 successful.

FIGURE 21-37 iMG/RG Wireless Tab

For iMG 1000 and iMG 2000 series devices, you must modify wireless settings from the iMG administration web interface; they cannot be configured directly in the NMS. Therefore, you must enable split management to configure wireless parameters for these devices.

The following rules apply for split management:

- When the iMG is configured as a routed service, local IP addresses are used to access the device.
- When the iMG is configured as a bridged service, the Internet IP address is used to access the device.
- For iMG634WA/B, iMG634WA/B-R2 and iMG616W devices there is rate limiting (upstream only) on wireless devices that are running software release 3-8 and higher. Rate limiting is controlled by the RG Internet profile (see iMG Internet Profile) or the iMG/RG - Internet Service tab on the Service Management form:



Customer ID: 634war2 iMG/RG IP Addr: 10.52.31.111 Video/Data Device: 10.52.30.34 Port: 10.8 POTS Device/Port: Unconfigured

iMG/RG Mgmt VC/VLAN: 7
TLS VC/VLAN: None
Video VC/VLAN: 40
Voice VC/VLAN: 10
PPPoE Connection State: N/A
Rate Limiting: Enabled
Up. Rate Limit (1..50000 kbps): 512
Up. Burst Size (1..67108 bps): 67108
Up. Scalar (1..100): 7
Down. Rate Limit (1..50000 kbps): 4096
Down. Burst Size (1..67108 bps): 67108
Down. Scalar (1..100): 33

Internet Service Profile: None
Internet Service Type: Routed Service
iMG/RG Internet VC/VLAN (2..4094 or None): 20
Use PPPoE: False
PPPoE User Name:
PPPoE Password:
TCP MSS Clamp: Disabled
Internet MTU (600..1500): 1500
iMG/RG Local Customer VLAN ID (2..4094): 2
Use DHCP to obtain WAN IP Address: True
DNS Servers (list of IP Addrs. or None): 10.52.201.64
Internet IP Address: 10.52.31.195
Internet Mask: 255.255.255.224
Local IP Address: 192.168.1.6
Local Mask: 255.255.255.0
Local DHCP Start IP Address: 192.168.1.10
Local DHCP End IP Address: 192.168.1.20

Thu Jun 20 09:25:12 EDT 2013 - Polling of RG_1339448555201 successful.

FIGURE 21-38 iMG Rate Limiting

21.14.6.1 Management Subnets

For iMG634WA/B, iMG634WA/B-R2 and iMG616W devices configured as a routed service:

- If a management subnet has previously been created, then when you enable split management the NMS automatically creates two management subnets: **nms** and **split_management**.

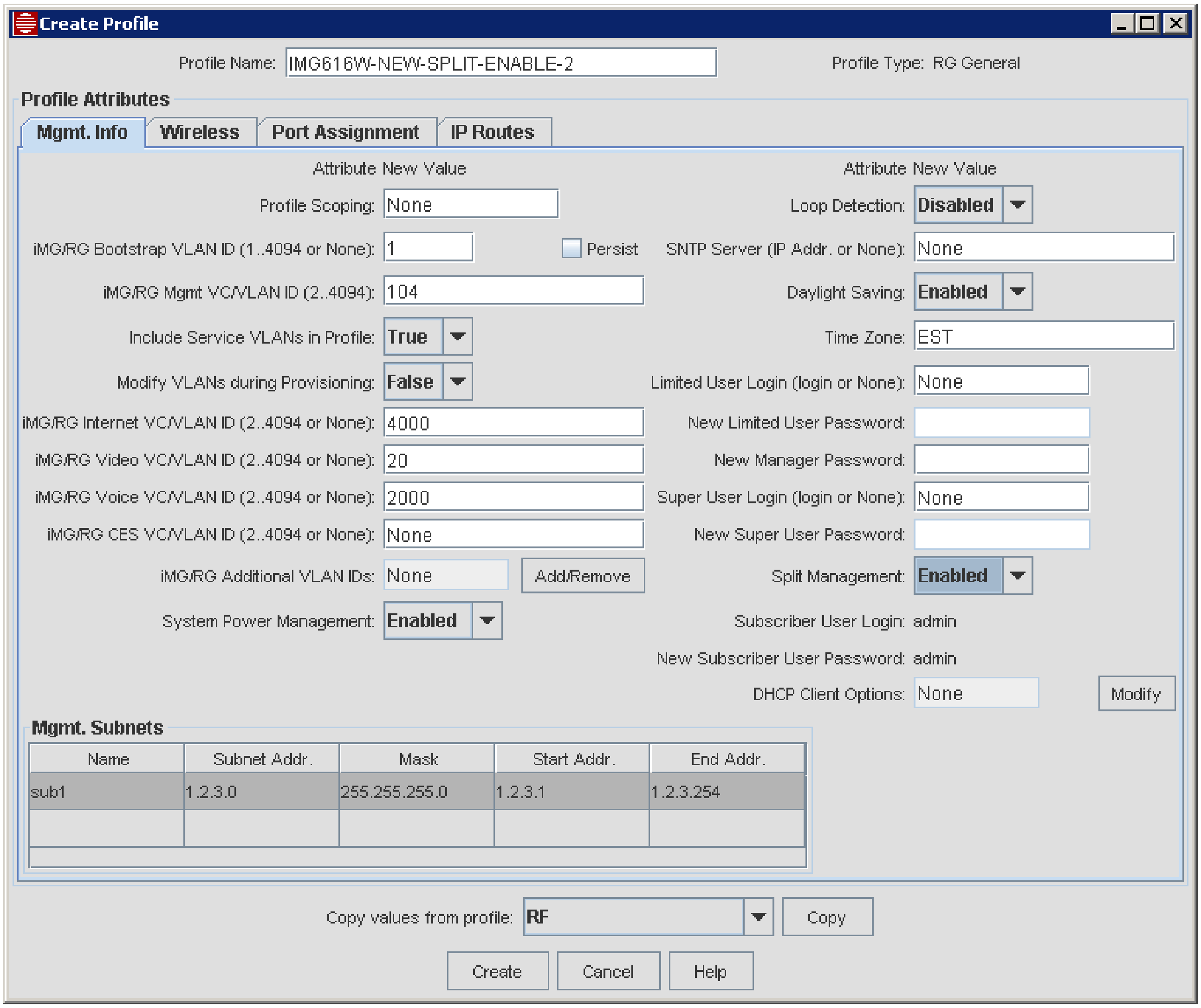
For iMG634WA/B, iMG634WA/B-R2 and iMG616W devices configured as a bridged service, only the **nms** subnet is created automatically; you must manually create the **split_management** subnet. To create the **split_management** subnet you will need the customer IP address, assigned by DHCP or a static address. The subscriber will need to know the iMG's SSID and the IP address for the wireless iMG.

21.14.6.2 Enabling Split Management in a Profile

To enable split management in a new profile:

1. In the **Network Objects** panel, go to **Network Service Data** > **Profiles**.
2. From the menu, go to **Network Services** > **Profile** > **iMG/RG Service Profiles** > **Create iMG/RG General Profile**. The **Create Profile** box for the RG General profile appears.
3. In the **Profile Name** field, enter a name for the profile.
4. Select the **Mgmt. Info** tab if it is not already selected.

5. In the **Split Management** drop-down list, select **Enabled**.



Create Profile

Profile Name: IMG616W-NEW-SPLIT-ENABLE-2

Profile Type: RG General

Profile Attributes

Attribute	New Value	Attribute	New Value
Profile Scoping:	None	Loop Detection:	Disabled
iMG/RG Bootstrap VLAN ID (1..4094 or None):	1 □ Persist	SNTP Server (IP Addr. or None):	None
iMG/RG Mgmt VC/VLAN ID (2..4094):	104	Daylight Saving:	Enabled
Include Service VLANs in Profile:	True	Time Zone:	EST
Modify VLANs during Provisioning:	False	Limited User Login (login or None):	None
iMG/RG Internet VC/VLAN ID (2..4094 or None):	4000	New Limited User Password:	
iMG/RG Video VC/VLAN ID (2..4094 or None):	20	New Manager Password:	
iMG/RG Voice VC/VLAN ID (2..4094 or None):	2000	Super User Login (login or None):	None
iMG/RG CES VC/VLAN ID (2..4094 or None):	None	New Super User Password:	
iMG/RG Additional VLAN IDs:	None	Split Management:	Enabled
System Power Management:	Enabled	Subscriber User Login:	admin
		New Subscriber User Password:	admin
		DHCP Client Options:	None

Mgmt. Subnets

Name	Subnet Addr.	Mask	Start Addr.	End Addr.
sub1	1.2.3.0	255.255.255.0	1.2.3.1	1.2.3.254

Copy values from profile: RF

FIGURE 21-39 iMG General Profile - Split Management

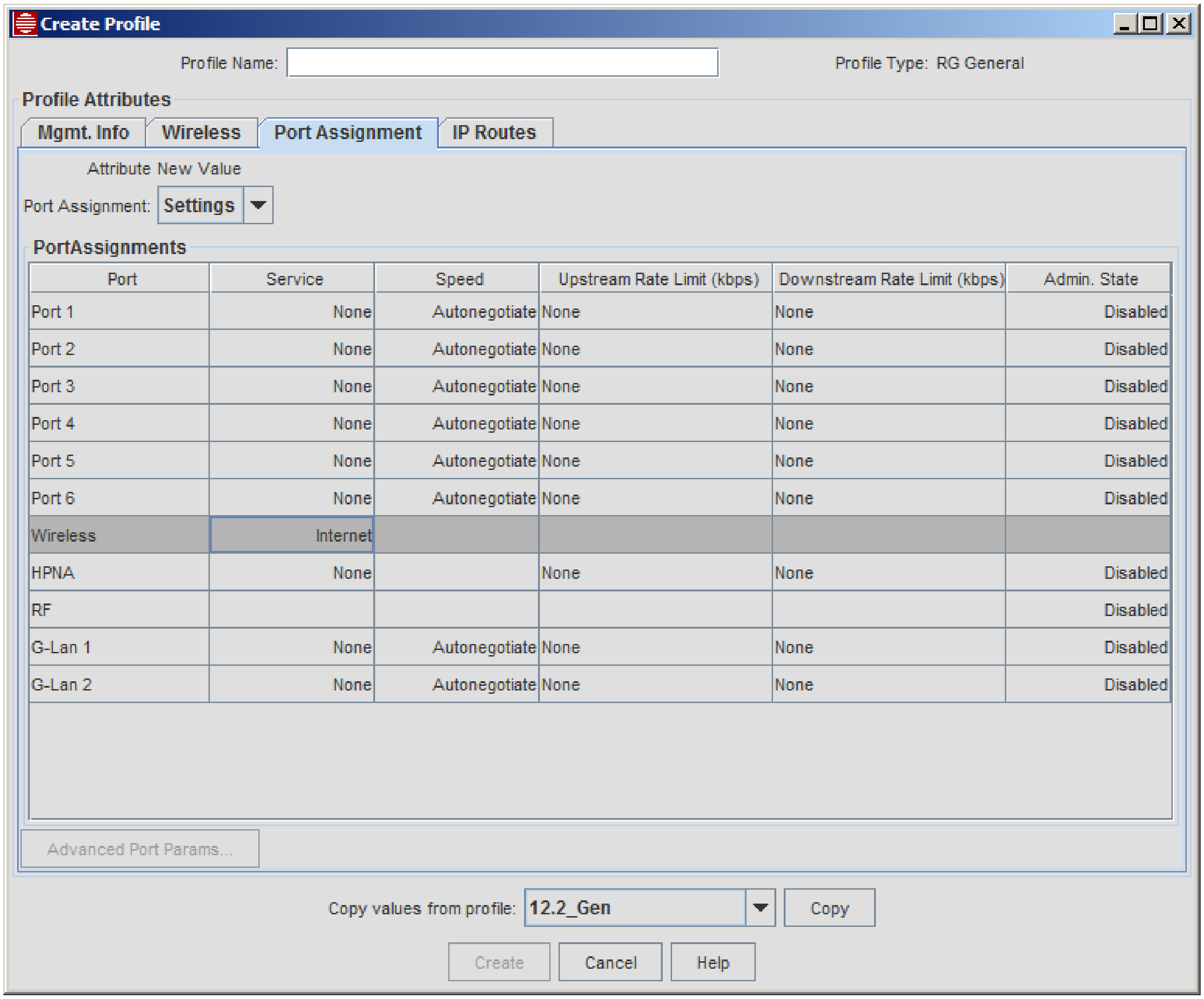
Note the default subscriber user login and password:

Subscriber User Login: **admin**

New Subscriber User Password: **admin**

The fields are read-only in the profile screen.

6. If you are setting up a profile for an iMG634WA/B, iMG634WA/B-R2 or iMG616W device you must also do the following:
   - Select the **Port Assignment** tab.
   - Select the **Wireless** port. In the **Service** drop-down list, select **Internet**.



Profile Name:

Profile Type: RG General

Port Assignment: Settings

Port	Service	Speed	Upstream Rate Limit (kbps)	Downstream Rate Limit (kbps)	Admin. State
Port 1	None	Autonegotiate	None	None	Disabled
Port 2	None	Autonegotiate	None	None	Disabled
Port 3	None	Autonegotiate	None	None	Disabled
Port 4	None	Autonegotiate	None	None	Disabled
Port 5	None	Autonegotiate	None	None	Disabled
Port 6	None	Autonegotiate	None	None	Disabled
Wireless	Internet				
HPNA	None		None	None	Disabled
RF					Disabled
G-Lan 1	None	Autonegotiate	None	None	Disabled
G-Lan 2	None	Autonegotiate	None	None	Disabled

Copy values from profile: 12.2_Gen

FIGURE 21-40 RG General Profile - Wireless port set to Internet

7. Click **Create** to create the profile.

21.14.6.3 Enabling Split Management on an Existing Device

When you provision a device, split management is disabled. You can enable split management in two ways:

- Modify the setting for the specific device, or,
- Modify the iMG General profile for the device and redeploy the profile to the device.

Note: *Allied Telesis recommends that you modify and redeploy the profile rather than change an attribute that is part of a deployed profile. Otherwise, the device will appear as out of sync with the profile.*

To modify the setting for a specific device:

1. In the **Network Objects** panel, go to **Network Inventory** > **iMG/RGs**.
2. In the **iMG/RGs** screen, right-click on the device and select **View/Modify Details**. The device service screen appears.
3. Select the **iMG/RG** tab, then select the **Mgmt. Info** tab.
4. In the **Split Management** drop-down list, select **Enabled**.

5. Click **Modify** to save the new settings.

To modify a profile:

1. In the **Network Objects** panel, go to **Network Service Data** > **Profiles**.
2. In the **Profiles** screen, right-click on the profile you want to modify and select **View Details**.
3. In the **Split Management** drop-down list, select **Enabled**.
4. Click **Modify** to save the new settings.

21.14.6.4 Using Split Management

When you enable split management, a subscriber can connect to the iMG over the iMG's administration web interface with the following credentials:

username: **admin**

password: **admin**

The username is set and cannot be changed. For security, subscribers should change the password the first time they log in.

When split management is enabled you can perform the following functions for subscribers:

- Reset the subscriber's password:
  1. In the **Network Objects** panel, go to **Network Inventory** > **iMG/RGs**.
  2. In the **iMG/RGs** screen, right-click on the device and select **View/Modify Details**. The device service screen appears.
  3. Select the **iMG/RG** tab, then select the **Mgmt. Info** tab.
  4. In the **New Subscriber User Password** drop-down list, select **admin**.
  5. Click **Modify** to save the new settings.
- Reset wireless parameters to default settings (iMG634WA/B, iMG634WA/B-R2 and iMG616W devices only):
  1. In the **Network Objects** panel, go to **Network Inventory** > **iMG/RGs**.
  2. In the **iMG/RGs** screen, right-click on the device and select **View/Modify Details**. The device service screen appears.
  3. Select the **iMG/RG** tab, then select the **Wireless** tab.
  4. Click **Reset Wireless Parameters**.

Note: You cannot reset iMG 1000 and iMG 2000 wireless parameters from the NMS.

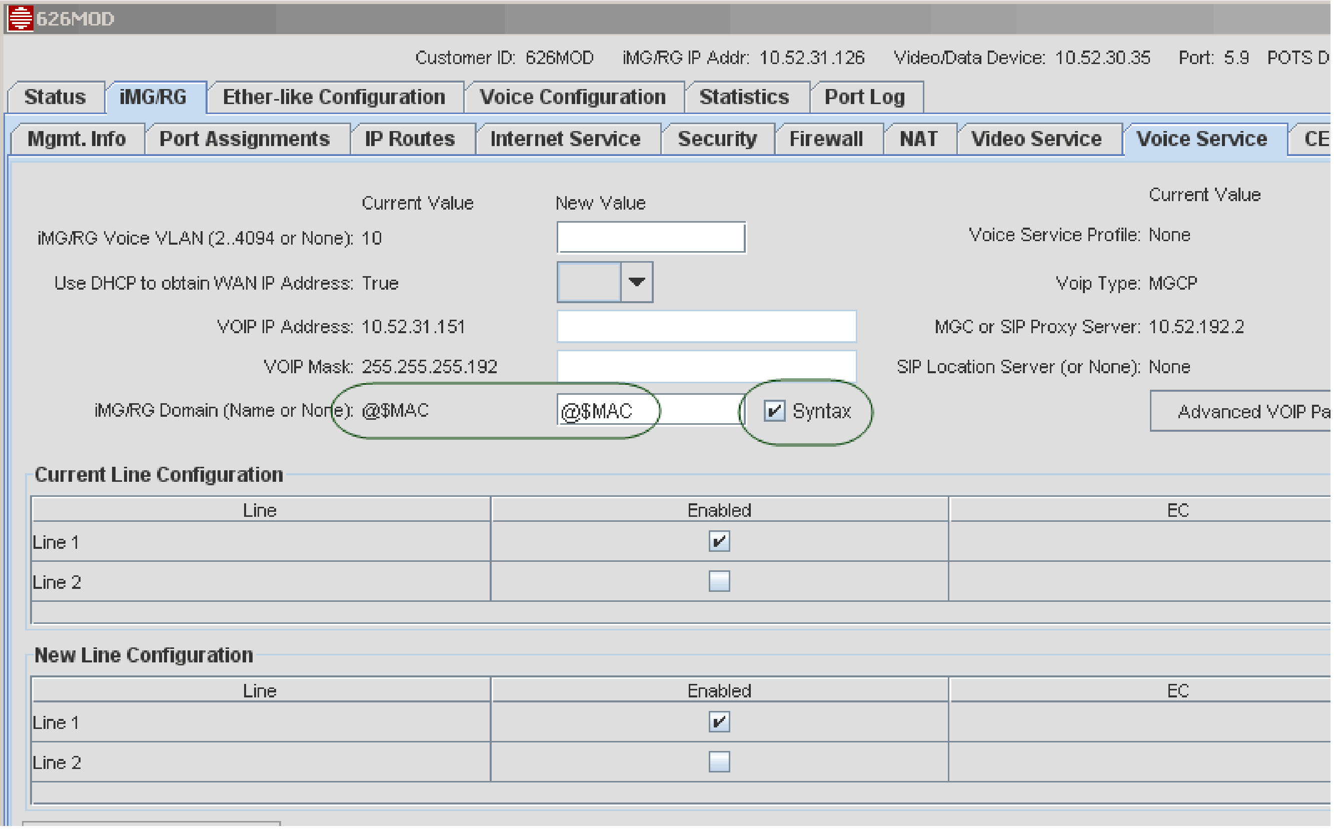
- Restore settings from the latest backup file.

  If there is a hardware replacement or a maintenance recovery scenario, you can restore the device's configuration settings to the latest backup file.

21.14.7 Changing VoIP Endpoint Syntax

For MGCP configurations that do not use GenBand, there is the option in the RG Voice profile to enter the VoIP endpoint that will be used. On the service management form for the iMG (iMG/RG -> Voice Service) there is the option of entering the endpoint syntax by selecting the Syntax checkbox and then filling in the iMG/RG Domain using the @ for the specific settings for the voice endpoint (@$IP, @$MAC, @$HOST, etc.). Refer to the following figure.

Note: The NMS supplies the "aaln/<telport number>"at the beginning of the string, and then the user continues the value with @. Therefore, values form vendors that do not follow this format are not supported, such as "$MAC:aaln/0@[$IP]". Modifying the end-point syntax is an advanced setting and should not be used unless required by the MGCP server.



Customer ID: 626MOD iMG/RG IP Addr: 10.52.31.126 Video/Data Device: 10.52.30.35 Port: 5.9 POTS D

	Current Value	New Value
iMG/RG Voice VLAN (2..4094 or None):	10	
Use DHCP to obtain WAN IP Address:	True	
VOIP IP Address:	10.52.31.151	
VOIP Mask:	255.255.255.192	
iMG/RG Domain (Name or None):	@$MAC	@$MAC ☑ Syntax

	Current Value
Voice Service Profile:	None
Voip Type:	MGCP
MGC or SIP Proxy Server:	10.52.192.2
SIP Location Server (or None):	None

Current Line Configuration

Line	Enabled	EC
Line 1	☑	
Line 2	☐	

New Line Configuration

Line	Enabled	EC
Line 1	☑	
Line 2	☐	

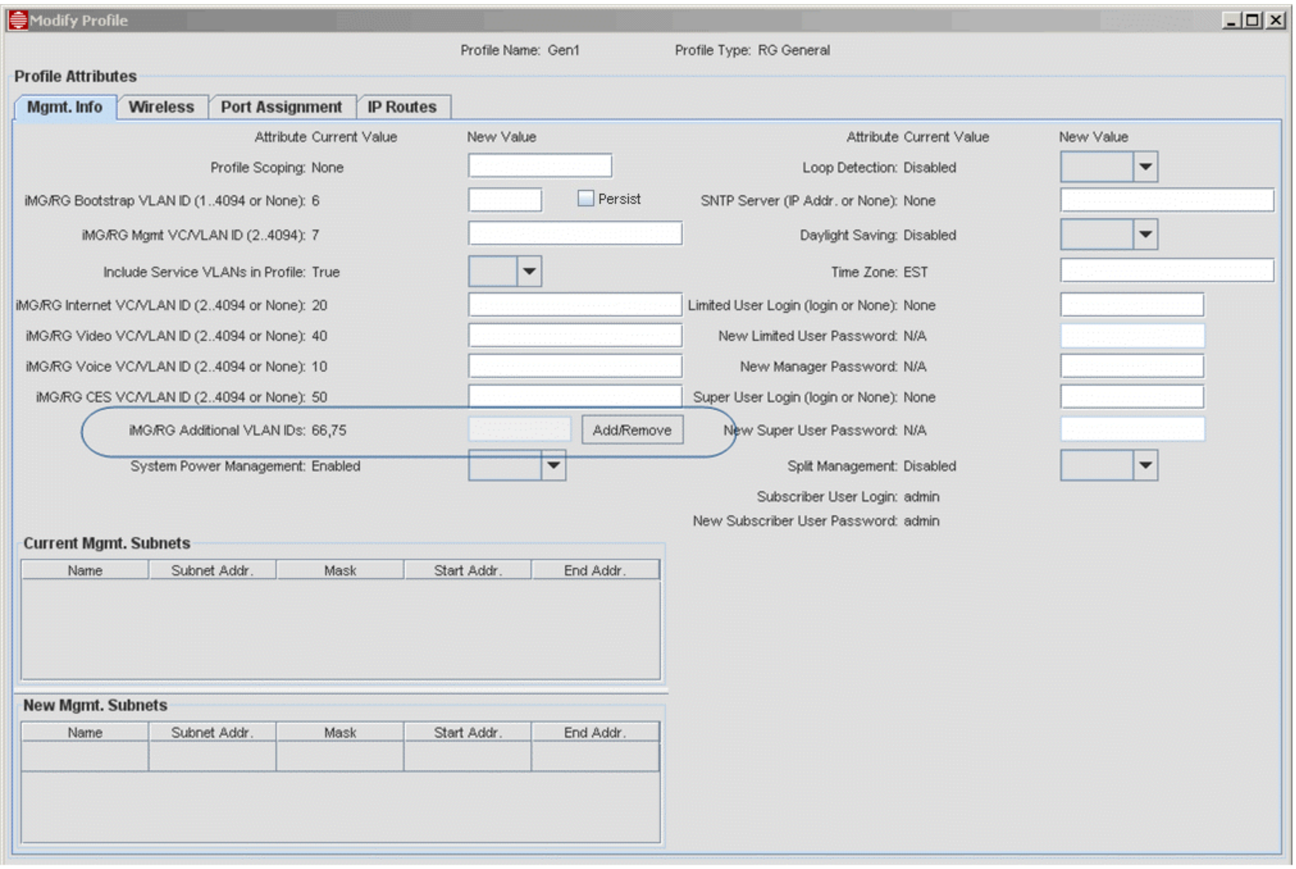
FIGURE 21-41 Setting VoIP Endpoint Syntax

21.14.8 Provisioning Custom VLANs

Although the RG General Profile is used to define VLANs for specific services, the iMG can support up to 14 VLANs. Each port can be connected to any VLAN in in any combination of tagged, untagged bridged and routed configurations.

Note: *When modular devices (iMG 726, iMG746, etc.) are used, one VLAN is used to manage HPNA and CES. Therefore, when the HPNA or CES card is provisioned, there is one less VLAN available.*

To allow for this, the RG General Profile can support these additional VLANs. Refer to the following figure.



Modify Profile

Profile Name: Gen1 Profile Type: RG General

Profile Attributes

Attribute	Current Value	New Value	Attribute	Current Value	New Value
Profile Scoping:	None		Loop Detection:	Disabled	
iMG/RG Bootstrap VLAN ID (1..4094 or None):	6	□ Persist	SNTP Server (IP Addr. or None):	None	
iMG/RG Mgmt VC/VLAN ID (2..4094):	7		Daylight Saving:	Disabled	
Include Service VLANs in Profile:	True		Time Zone:	EST	
iMG/RG Internet VC/VLAN ID (2..4094 or None):	20		Limited User Login (login or None):	None	
iMG/RG Video VC/VLAN ID (2..4094 or None):	40		New Limited User Password:	N/A	
iMG/RG Voice VC/VLAN ID (2..4094 or None):	10		New Manager Password:	N/A	
iMG/RG CES VC/VLAN ID (2..4094 or None):	50		Super User Login (login or None):	None	
iMG/RG Additional VLAN IDs:	66,75	Add/Remove	New Super User Password:	N/A	
System Power Management:	Enabled		Split Management:	Disabled	
			Subscriber User Login:	admin	
			New Subscriber User Password:	admin	

Current Mgmt. Subnets

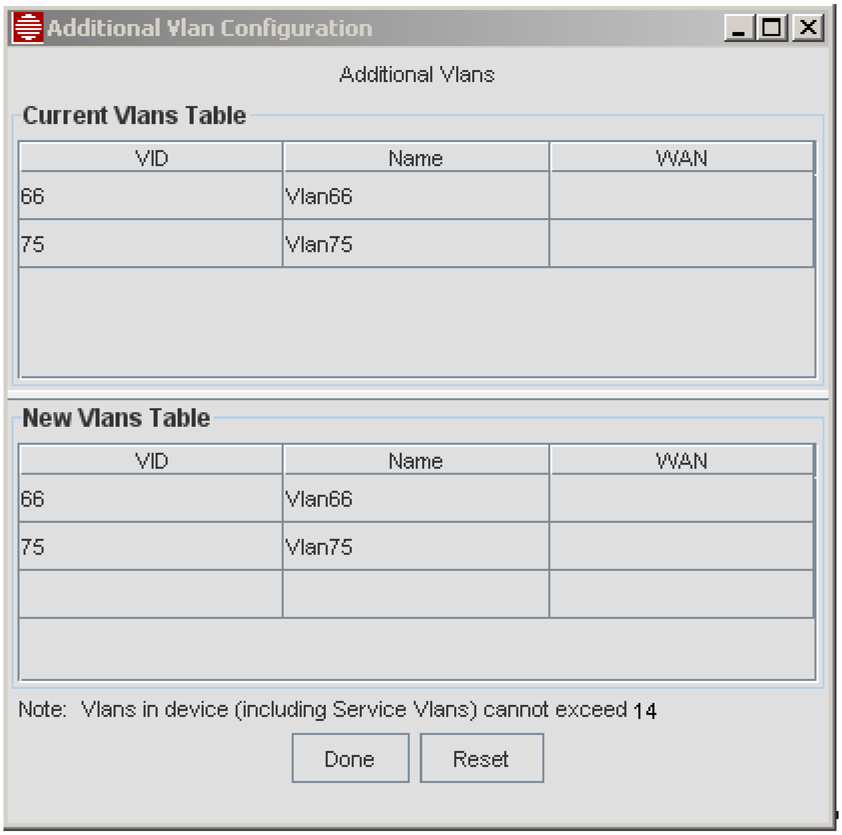
Name	Subnet Addr.	Mask	Start Addr.	End Addr.

New Mgmt. Subnets

Name	Subnet Addr.	Mask	Start Addr.	End Addr.

FIGURE 21-42 RG General Profile - Additional VLANs

The Add/Remove button allows the user to create or modify the additional VLANs in iMG. Refer to the following figure.



VID	Name	WAN
66	Vlan66	
75	Vlan75	

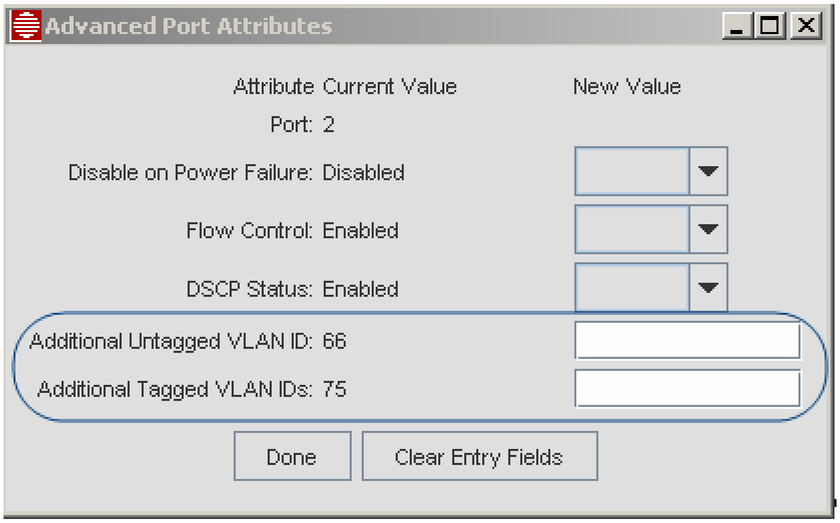
VID	Name	WAN
66	Vlan66	
75	Vlan75	

Note: Vlans in device (including Service Vlans) cannot exceed 14

FIGURE 21-43 Panel to Add/Remove/Modify Custom VLANs (Once Profile is Created)

This panel includes the name and indication if the VLAN is tagged on WAN port. The table format used works similar to others in NMS where the top table shows current values and the bottom table is for editing. Since iMGs cannot have more than 14 VLANs, this will limit the number of VLANs in device to 14 (including Default and all service VLANs).

Also to support the custom VLANs, the Advanced parameters panel on the iMG/RG Service Management Panel *(iMG/RG->Port Assignments)* for LAN ports includes fields that allow the user to specify untagged VLAN ID or tagged VLAN IDs on the selected port. These VLANs specified must be those that were created as additional VLANs (not service VLANs) and are only allowed if the LAN port is not associated to any other service (set to None). This is done to protect existing services from being affected by configuration or traffic that may be sent through additional VLANs. Refer to the following figure.



Attribute Current Value New Value

Port: 2

Disable on Power Failure: Disabled

Flow Control: Enabled

DSCP Status: Enabled

Additional Untagged VLAN ID: 66

Additional Tagged VLAN IDs: 75

FIGURE 21-44 Advanced Port Attributes - Custom VLANs

21.14.9 Error Conditions when Provisioning

21.14.9.1 Access Island and Open Access

Since provisioning each model involves a different VLAN configuration, the following steps will produce an error message:

- In both the RG General Profile and Service Profiles no service VLANs are datafilled
- There is conflict between the VLAN configuration in the iMG/RG General Profile and in the Service Profiles
- The Profiles and provisioned VLANs don't match, and so the iMG/RG in the Inventory table will have a * under the appropriate Profile

21.15 iMG Installation Procedures

With the use of profiles and DHCP, the installation, reconfiguration, and de-installation of iMGs/RGs does not involve complex (and therefore error-prone) procedures. These procedures can be grouped into two main areas:

1. Installing, reconfiguring, and removing the iMG/RG using the NMS
2. Changing an iMG/RG that was not configured using the NMS to one that does

In the first area, the initial installation of an iMG/RG (out of the box) includes most of the steps that are needed when reconfiguring or removing the iMG/RG, in a different sequence.

A special procedure is the changing of the Customer ID, since certain steps must be followed to ensure the ID has been changed. Refer to Changing a Customer ID.

Note: *The procedures here will assume that the user is performing these procedures for the Access Island. Whenever there is a change in a step needed to accommodate the open Access model, this change will be highlighted.*

Note: *The NMS supports translations on the iMAP ports. For all of the following procedures, if the procedure includes adding a translation (or translations) to the iMG/RG configuration, the iMAP port profile that includes the translation must be applied before changes are made to the iMG/RG profiles.*

21.15.1 Installation Restrictions

21.15.1.1 Initial and Subsequent “push down” of Configuration Data

When provisioning the RG from the AlliedView NMS, there is the initial sequence of:

1. Pre-provisioning (ports, profiles)
2. Discovery (DHCP)
3. the “pushing down” of the initial configuration data.

It is important to note that once this data is pushed down, subsequent discoveries of the RG by the AlliedView NMS (usually every 24 hours) do not include a subsequent pushing down of this data if there has been a change in the iMG/RG configuration since the last discovery. If changes have been made to the iMG/RG configuration (such as a change in profile), the AlliedView NMS will make only the changes to the iMG/RG necessary to reflect the new configuration.

Note: This is in contrast to other methods (ZTC) where the configuration server stored the iMG/RG configuration. The iMG/RG would query the ZTC if there had been a change made on the ZTC server; if there had been a change, the ZTC would reconfigure the iMG/RG and upon reboot the changes would take effect.

Moreover, the behavior of the AlliedView NMS is that if the pushing down of **initial** configuration data fails (perhaps due to a network fault), the AlliedView NMS raises an alarm. The user can then:

- Wait 24 hours for the next discovery (or more if there are many devices)
- Perform a manual discovery

In either scenario, the AlliedView NMS will try to push down the configuration data.

The important concept is that **the AlliedView NMS does not try to push down the configuration data unless this is for new hardware**. This leads to the next subsection.

21.15.1.2 Moving the iMG/RG to another Port (Re-provisioning)

An administratively efficient way to provision the iMG/RG is by using Access Islands, with each Access Island having its own unique set of VLANs. This makes moving an iMG/RG from one port to another behave as follows:

- If the user moves an already provisioned iMG/RG from one iMAP port to another in the **same** Access Island, the AlliedView will treat the iMG/RG as new hardware and will de provision and re-provision the RG, using data for that new port.
- If the user moves the already provisioned iMG/RG from one iMAP port to another in a **different** Access Island, the AlliedView NMS won’t see the RG because it is not the correct RGMgmt VLAN (and IP address) for that Access Island. In this scenario, the user should telnet to the iMG/RG before removing the iMG/RG and set the iMG/RG back to its factory settings. Then, when moving the iMG/RG to the new port in the different Access Island, DHCP discovery will start with the RG’s default VLAN and go through the process of finding and then using the RGMgmt VLAN for that new Access Island.

21.15.2 Pre-provision Future Customer (Provision iMAP Port, no Services)

21.15.2.1 When to use this Procedure

- The administrator wishes to provision the iMAP port with the iMG/RG, and not provision any specific services. (An example would be for a vacant residence.)
- Services will be added later.

21.15.2.2 Pre-requisite Procedures

Before performing this procedure, the administrator should have already done the following:

- Have an iMG/RG General Profile with a name such as “DVLK-AI01-Vacant” and include scoping so that when it is used only iMAPs from AI01 are accessible. Refer to Figure 21-45, Figure 21-46, and Figure 21-47.

Note: For Open Access, the Profile Name could be “DVLK-Vacant” since the Access Island number is not used as part of Scoping.

- Have a port profile available that reflects the type of port and the capabilities desired, such as “DVLK-AI01-100Mbps”.

Note: In this profile, the VLAN Configuration is not included.

- Have a customer ID ready that reflects administrative naming conventions for this type of provisioning. An appropriate ID would be the residence address.

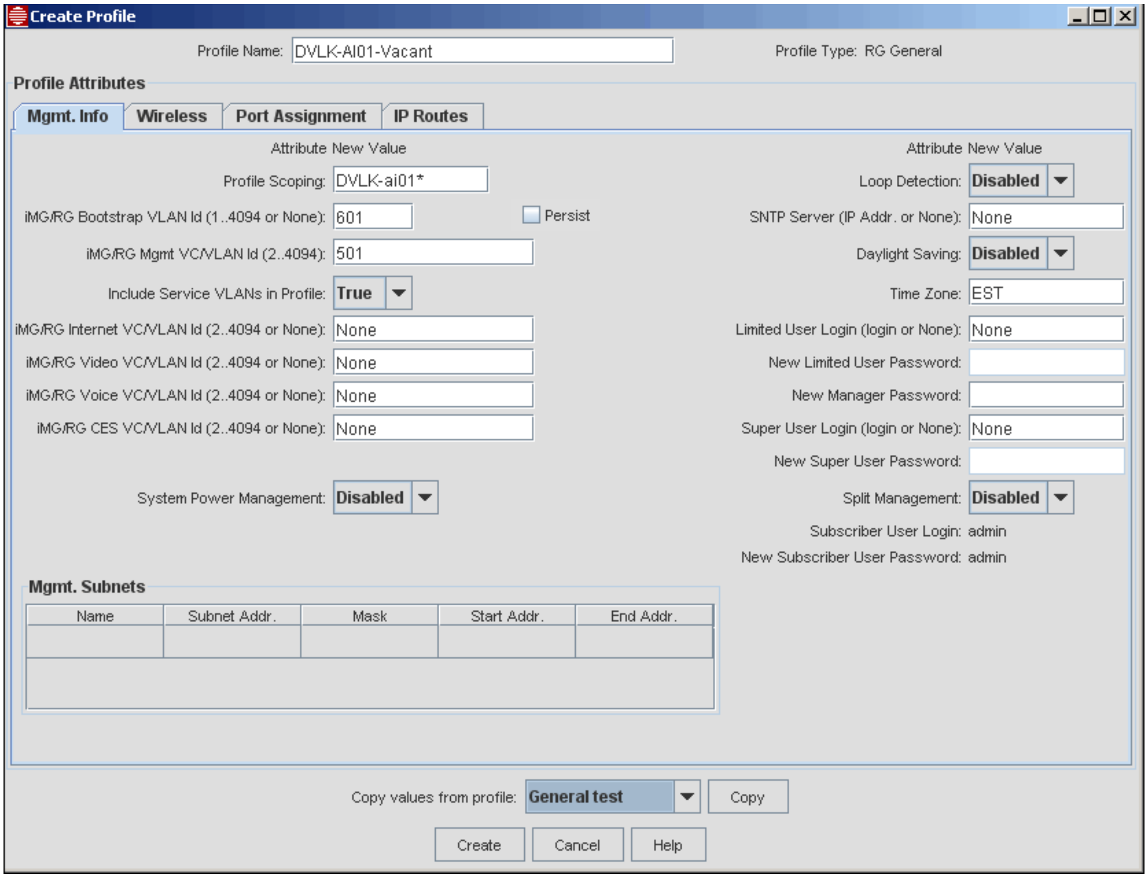
21.15.2.3 Pre-provision the Customer

Using the sample names listed above, the following steps are performed:

1. Bring up the Provision New Triple Play Customer Form using one of these methods:

- From the main AlliedView NMS menu, select *Tools -> Customer Management -> Add New Triple Play Customer*.
- For an iMAP icon, select *Provision -> Port Management*. From the Port Management Form select the port for the work order, which will have no Customer ID, and click **Provision New Customer/Port**. (An already provisioned port should always have a Customer ID.)
- From the port table in Network Inventory, right-click the port from the work order and select **Provision New Customer/Port**.

2. In the Provision New Triple Play Customer Form, enter a Customer ID, in this example the residence address.
3. Click on **Add Customer Info** to add the additional text.
4. Select the iMG/RG General Profile, in this case “DVLK-AI01-Vacant”. Because of scoping, only those devices from Access Island 1 are available.
5. Enter a port Profile. Only those port profiles relevant for the type of port selected are available.
6. Review the filled out form, as shown in Figure 21-48.



Create Profile

Profile Name: DVLK-AI01-Vacant

Profile Type: RG General

Profile Attributes

Attribute	New Value
Profile Scoping:	DVLK-ai01*
iMG/RG Bootstrap VLAN Id (1..4094 or None):	601 □ Persist
iMG/RG Mgmt VC/VLAN Id (2..4094):	501
Include Service VLANs in Profile:	True
iMG/RG Internet VC/VLAN Id (2..4094 or None):	None
iMG/RG Video VC/VLAN Id (2..4094 or None):	None
iMG/RG Voice VC/VLAN Id (2..4094 or None):	None
iMG/RG CES VC/VLAN Id (2..4094 or None):	None
System Power Management:	Disabled

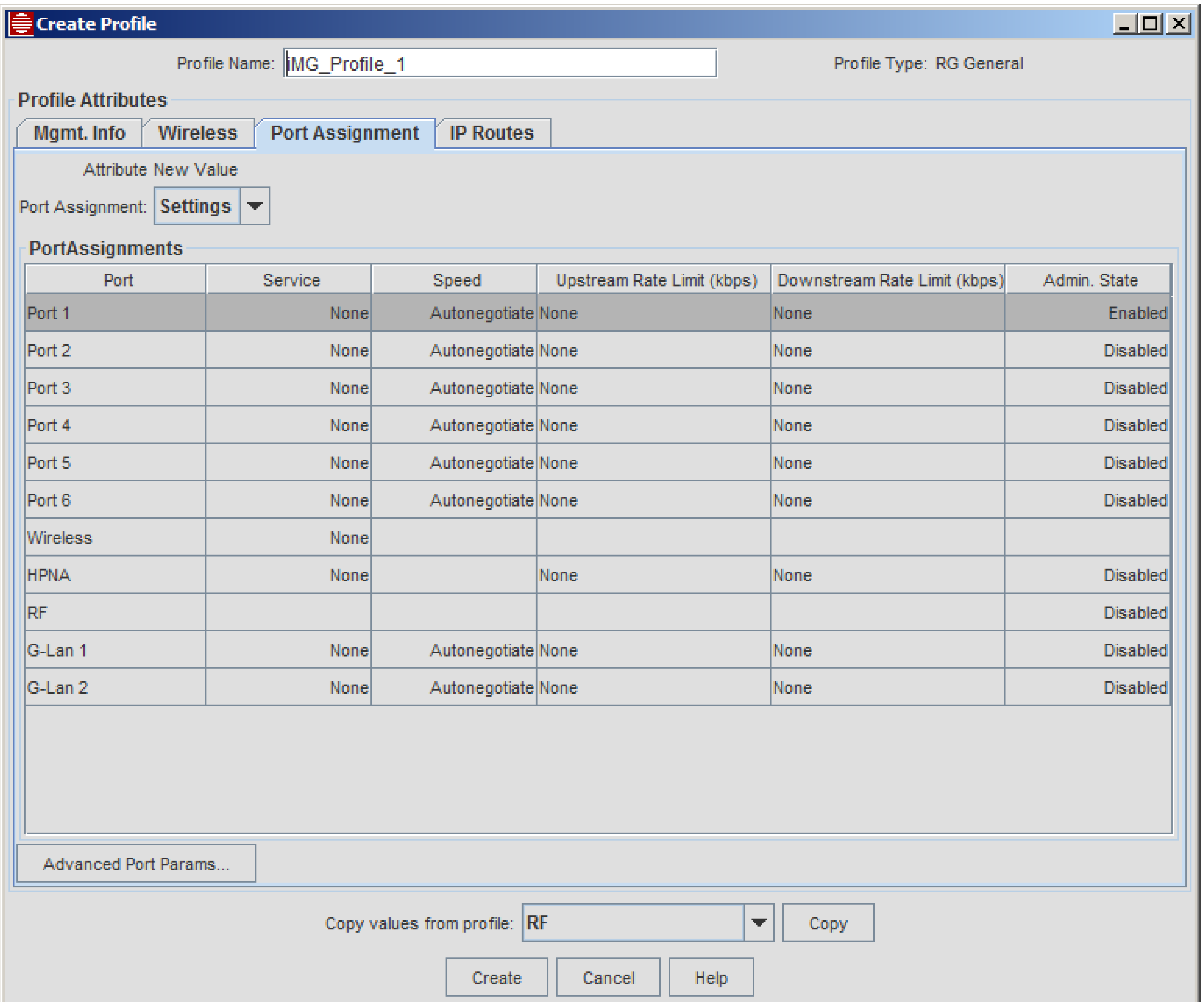
Attribute	New Value
Loop Detection:	Disabled
SNTP Server (IP Addr. or None):	None
Daylight Saving:	Disabled
Time Zone:	EST
Limited User Login (login or None):	None
New Limited User Password:	
New Manager Password:	
Super User Login (login or None):	None
New Super User Password:	
Split Management:	Disabled
Subscriber User Login:	admin
New Subscriber User Password:	admin

Mgmt. Subnets

Name	Subnet Addr.	Mask	Start Addr.	End Addr.

Copy values from profile: General test

FIGURE 21-45 Profile for DVLK-AI01-Vacant - Mgmt Info



Create Profile

Profile Name: iMG_Profile_1

Profile Type: RG General

Profile Attributes

Attribute New Value

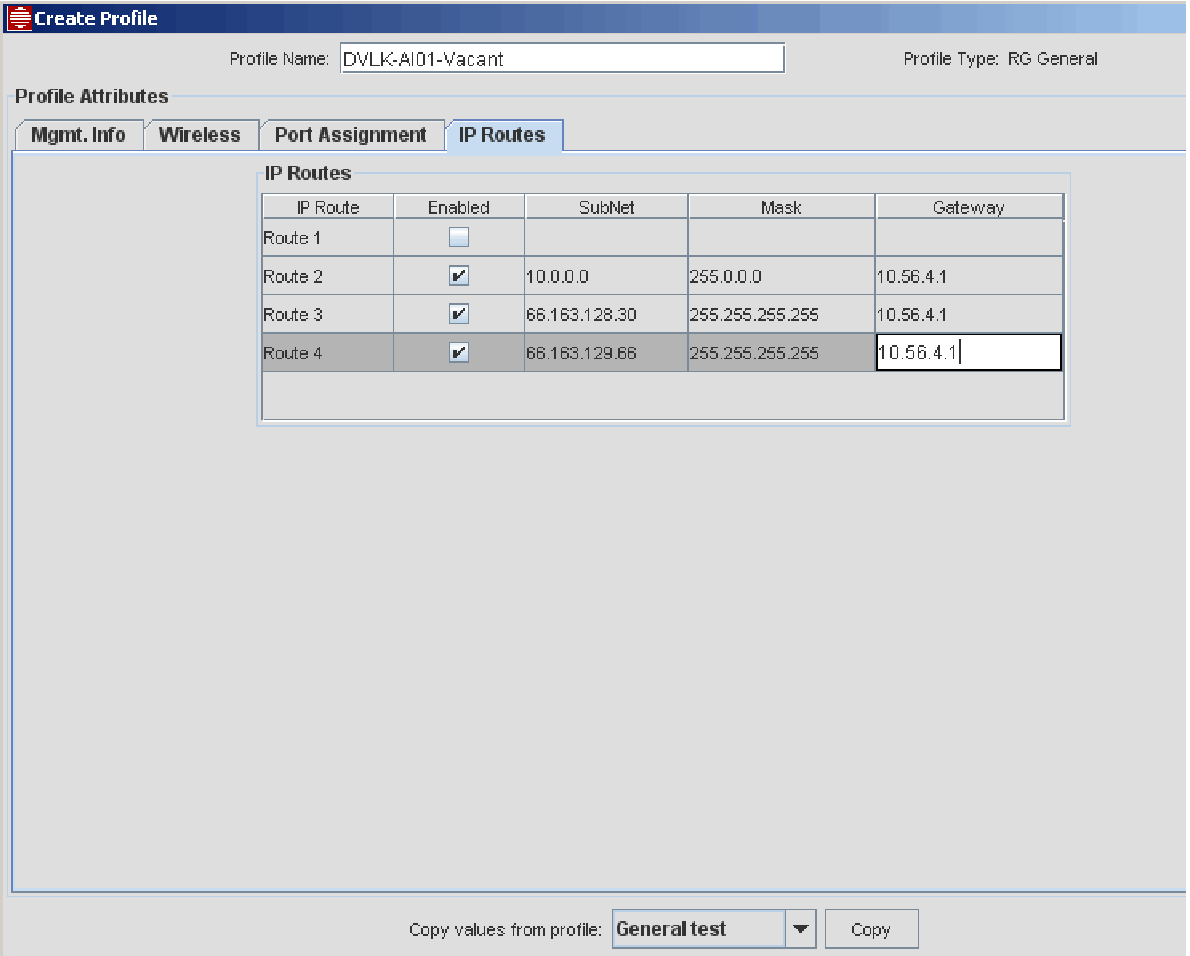
Port Assignment: Settings

PortAssignments

Port	Service	Speed	Upstream Rate Limit (kbps)	Downstream Rate Limit (kbps)	Admin. State
Port 1	None	Autonegotiate	None	None	Enabled
Port 2	None	Autonegotiate	None	None	Disabled
Port 3	None	Autonegotiate	None	None	Disabled
Port 4	None	Autonegotiate	None	None	Disabled
Port 5	None	Autonegotiate	None	None	Disabled
Port 6	None	Autonegotiate	None	None	Disabled
Wireless	None				
HPNA	None		None	None	Disabled
RF					Disabled
G-Lan 1	None	Autonegotiate	None	None	Disabled
G-Lan 2	None	Autonegotiate	None	None	Disabled

Copy values from profile: RF

FIGURE 21-46 Profile for DVLK-AI01-Vacant - Port Assignment



Create Profile

Profile Name: DVLK-AI01-Vacant

Profile Type: RG General

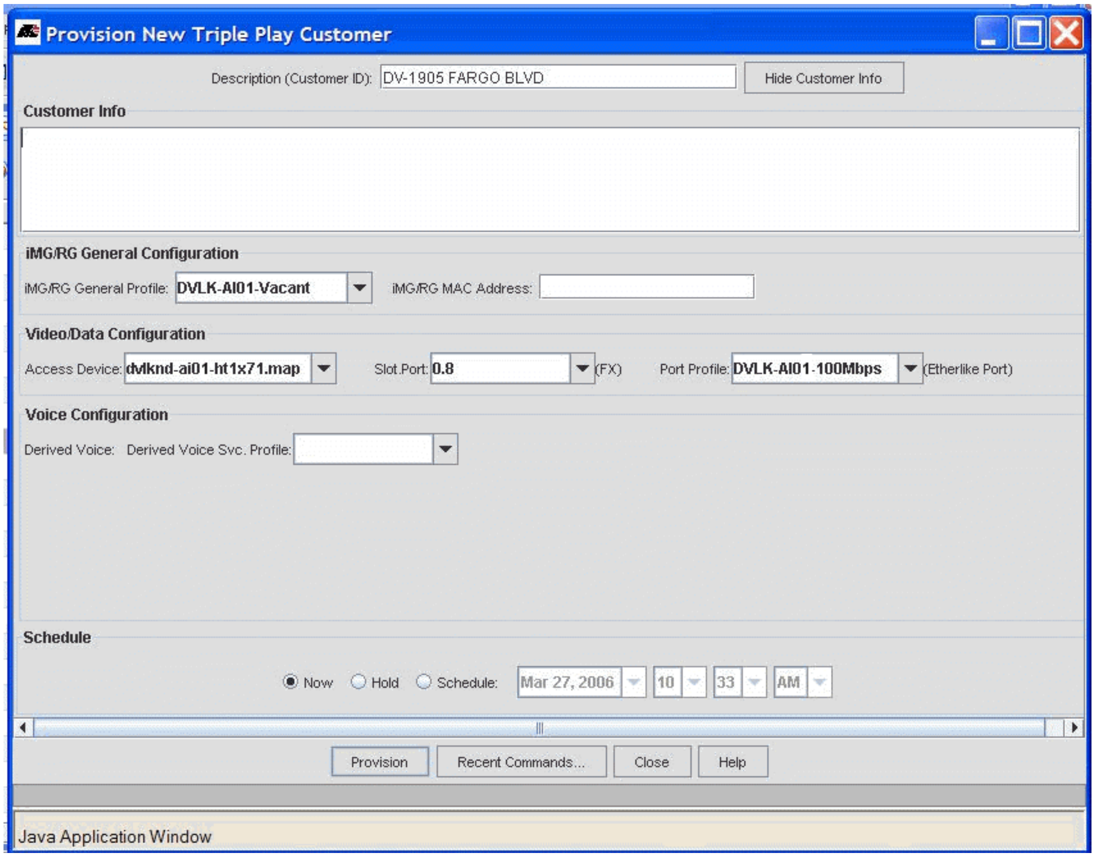
Profile Attributes

IP Routes

IP Route	Enabled	SubNet	Mask	Gateway
Route 1	□			
Route 2	☑	10.0.0.0	255.0.0.0	10.56.4.1
Route 3	☑	66.163.128.30	255.255.255.255	10.56.4.1
Route 4	☑	66.163.129.66	255.255.255.255	10.56.4.1

Copy values from profile: General test

FIGURE 21-47 Profile for DVLK-AI01-Vacant - IP Routes



Description (Customer ID): DV-1905 FARGO BLVD

Customer Info

iMG/RG General Configuration

iMG/RG General Profile: DVLK-AI01-Vacant iMG/RG MAC Address:

Video/Data Configuration

Access Device: dvlknd-ai01-ht1x71.map Slot.Port: 0.8 (FX) Port Profile: DVLK-AI01-100Mbps (Etherlike Port)

Voice Configuration

Derived Voice: Derived Voice Svc. Profile:

Schedule

● Now ○ Hold ○ Schedule: Mar 27, 2006 10 33 AM

FIGURE 21-48 Provision Triple Play - No Services

21.15.2.4 Add Services to an Already Provisioned Port

When services must be added to the pre-provisioned port, the same steps are used when adding services to a port that already has some service(s) configured, using the View/Modify Customer window. Following is a summary of these steps. For details, refer to the procedures in the rest of this Subsection.

1. Select the appropriate new **general** profile that reflects the services desired and then **Modify**.
2. Select the appropriate **internet** profile then **Modify**. (if services required)
3. Select the appropriate **video** profile and **Modify**. (if services required)
4. Select the appropriate **voice** profile and **Modify**.
5. From the view/modify status tab **Add a derived voice line**
6. Select **Save the Config** and **Restart**.

21.15.3 Provision a new Customer (out of the box) - Triple Play

21.15.3.1 When to use this Procedure

- The iMAP port that interfaces the iMG/RG has not been created.
- Customer has purchased video, data, and derived voice service.
- The customer/installer will remove an iMG/RG from its packaging and so all settings are at factory defaults.

21.15.3.2 Pre-requisite Procedures

Before performing this procedure, the user should have already done the following:

1. At the iMAP, ensure the following are already configured:

- VLANs for DHCP and services have been created.
- The iMAP card/port that interfaces the iMG/RG has been installed and enabled.

2. User has work order that should include the following:

- Attributes that will be used for GenBand configuration

3. All appropriate profiles are defined. The following profiles are used:

Note: *For Open Access, the General Profile would not have service VLANs defined, while the service-specific Profiles would have VLANs.*

TABLE 21-7 **Example Profiles for Initial Configuration**

Profile Type	Example Profile Name	Description
Upstream Port Profile		Used for Fast Ethernet Ports
RG General Profile	"DeskLab-3Play-1Video"	Example profile that has all three services and supports only one STB.
RG Internet Profile	"HomeNetworkInet""	
RG Video Profile	"Video-Proxy"	For video proxy service
RG Derived Voice Profile	"VOIPPhone"	For derived voice profile
Line Profile	g711_mulaw_10	Used in conjunction with G6 and G2

21.15.3.3 Provision the iMAP Port (Triple Play Form)

Datafilling the Triple Play form allows the user to create a unique Customer ID and to associate this with all the relevant profiles. Follow these steps:

1. Bring up the Provision New Triple Play Customer Form using one of these methods:

- From the main AlliedView NMS menu, select *Tools -> Customer Management -> Add New Triple Play Customer.*
- For an iMAP icon, select *Provision -> Port Management*. From the Port Management Form select the port for the work order, which will have no Customer ID, and click **Provision New Customer/Port**. (An already provisioned port should always have a Customer ID.)
- From the port table in Network Inventory, right-click the port from the work order and select **Provision New Customer/Port**.

2. In the Provision New Triple Play Customer Form, enter a Customer ID
3. Click on Add Customer Info to add the additional text to define this customer.

   Refer to Naming Convention for Customer IDs (Triple Play Form) for suggestions on naming conventions for Customer ID and Customer Info.

4. Enter the iMG/RG General Profile **DeskLab-3Play-1Video** from the pull-down.
5. If necessary, enter the Access Device and Slot.Port. See the note below on scoping.

Note: *With scoping, if the Triple-Play Form is brought up without an Access Device and Slot.port, only those devices that use the General Profile are available. Conversely, the user could choose a device first, and only those profiles available for that device are shown.*

6. Enter a port Profile. Only those port profiles relevant for the type of port are available.

7. Select an Internet Svc. Profile, in this case **HomeNetworkInet.**

   Note that the Local IP Addr, Mask, and DHCP Start/End addresses are datafilled.

8. Select an Video Svc. Profile, in this case **Video-Proxy.**

   Note that the Local IP Addr, Mask, and DHCP Start/End addresses are datafilled.

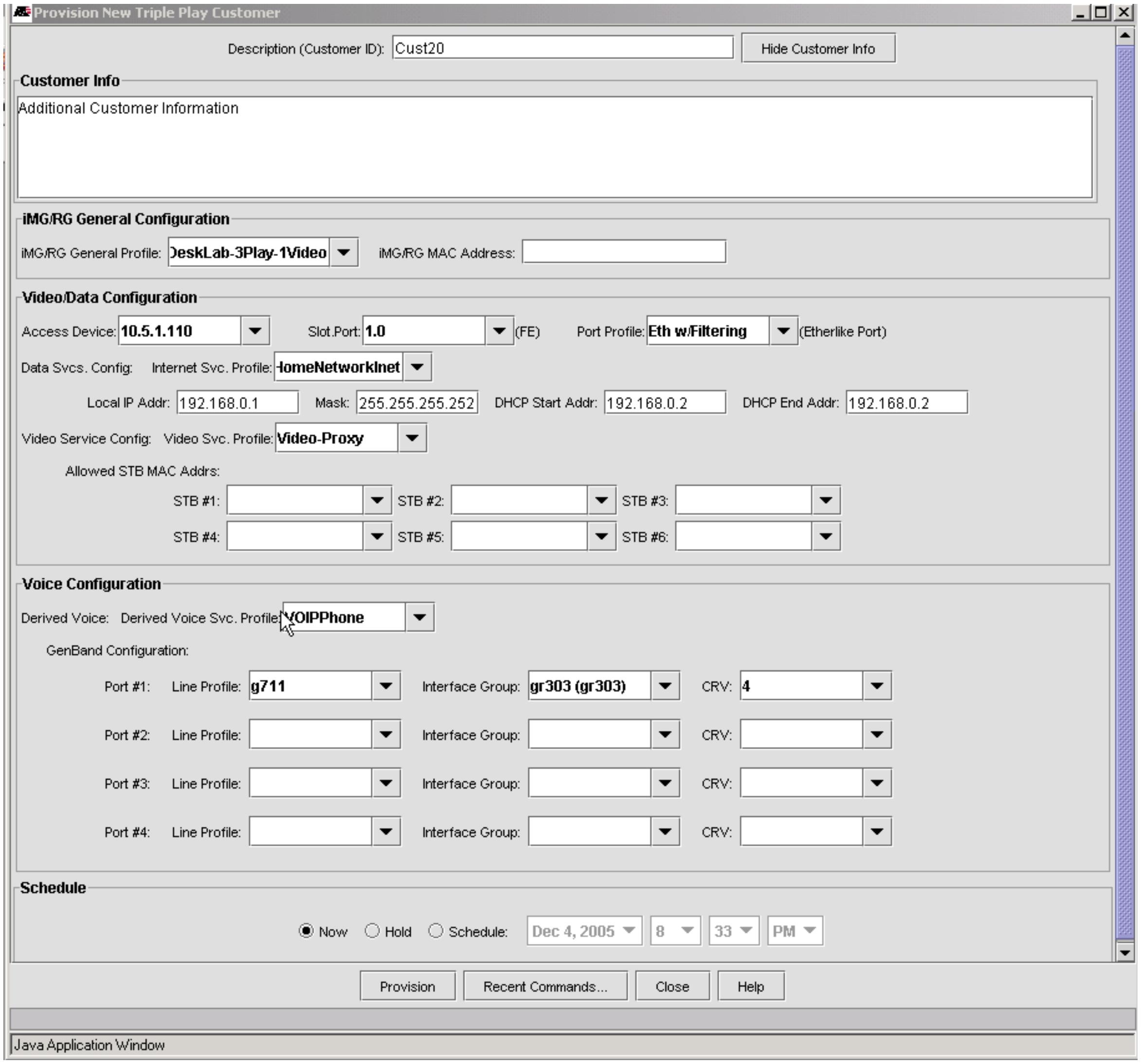
9. Select a Derived Voice Svc. Profile, in this case **VOIPPhone.**

   Note that the GenBand Configuration fields are now available.

10. Enter the GenBand Configuration attributes for Port #1, the Line Profile, the Interface Group, and CRV.

    These values should be taken from the work order.

11. Review the filled out form, as shown in Figure 21-49.



Provision New Triple Play Customer

Description (Customer ID): Cust20

Customer Info

Additional Customer Information

iMG/RG General Configuration

iMG/RG General Profile: DeskLab-3Play-1Video iMG/RG MAC Address:

Video/Data Configuration

Access Device: 10.5.1.110 Slot.Port: 1.0 (FE) Port Profile: Eth w/Filtering (Etherlike Port)

Data Svcs. Config: Internet Svc. Profile: HomeNetworkInet

Local IP Addr: 192.168.0.1 Mask: 255.255.255.252 DHCP Start Addr: 192.168.0.2 DHCP End Addr: 192.168.0.2

Video Service Config: Video Svc. Profile: Video-Proxy

Allowed STB MAC Addrs:

STB #1: STB #2: STB #3:

STB #4: STB #5: STB #6:

Voice Configuration

Derived Voice: Derived Voice Svc. Profile: VOIPPhone

GenBand Configuration:

Port #1: Line Profile: g711 Interface Group: gr303 (gr303) CRV: 4

Port #2: Line Profile: Interface Group: CRV:

Port #3: Line Profile: Interface Group: CRV:

Port #4: Line Profile: Interface Group: CRV:

Schedule

● Now ○ Hold ○ Schedule: Dec 4, 2005 8 33 PM

FIGURE 21-49 Completed Triple Play Form - With Services

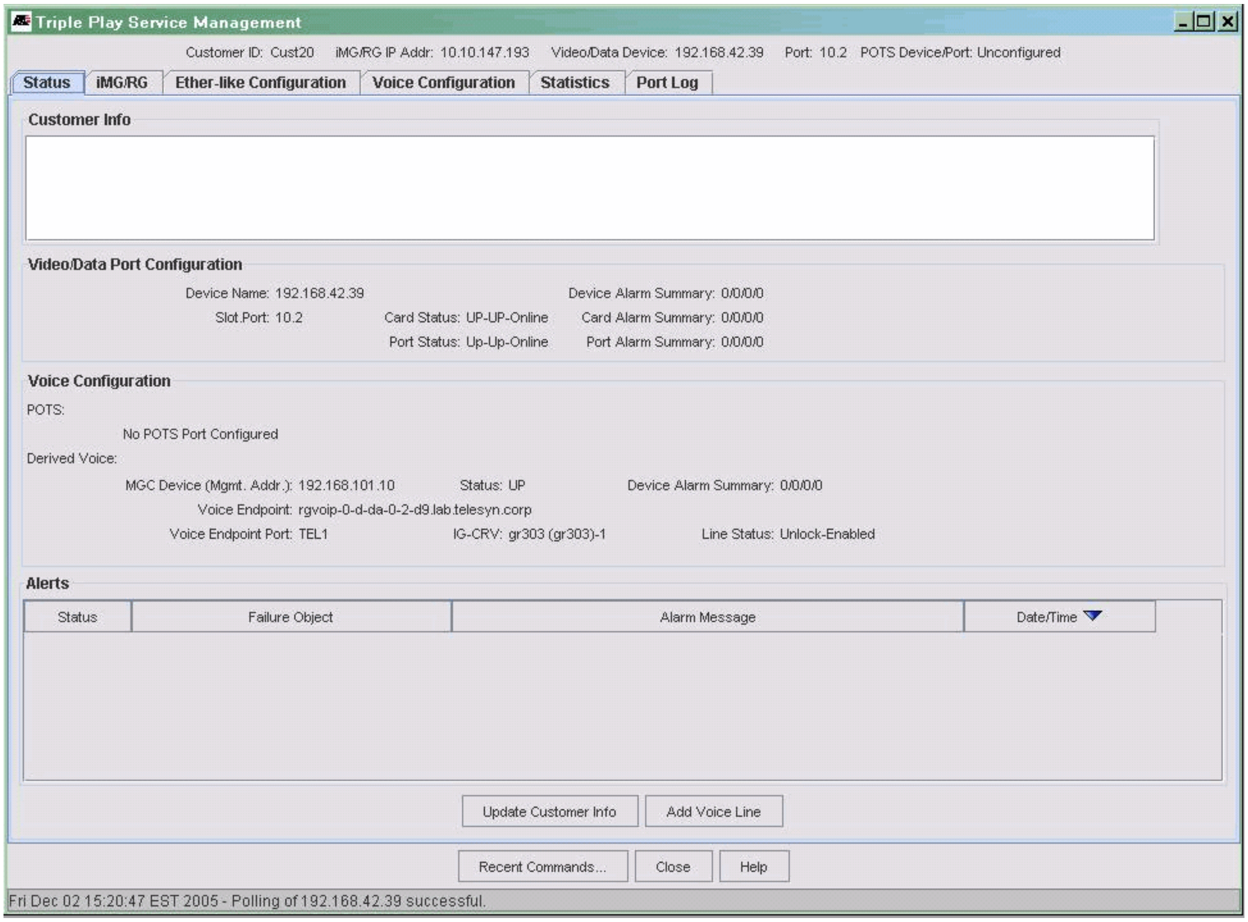
12. Invoke the Triple-Play form to provision the port.

- To provision now, click on Provision. The Task Details screen appears and shows progress states. If there is a failure, double-click on the relevant sub-task for details.

- To provision, select Hold and then Provision.
- To provision at set time, click on Schedule, enter the date/time, and then Provision

Note: At this point, the user can provision other ports, since the iMG/RG has not been connected to the iMAP; all that is being provisioned is the iMAP port.

13. Review the Triple Play Service Management Form, as shown in Figure 21-50.



Customer ID: Cust20 iMG/RG IP Addr: 10.10.147.193 Video/Data Device: 192.168.42.39 Port: 10.2 POTS Device/Port: Unconfigured

Customer Info

Video/Data Port Configuration

Device Name: 192.168.42.39 Device Alarm Summary: 0/0/0/0
Slot.Port: 10.2 Card Status: UP-UP-Online Card Alarm Summary: 0/0/0/0
Port Status: Up-Up-Online Port Alarm Summary: 0/0/0/0

Voice Configuration

POTS:
No POTS Port Configured
Derived Voice:
MGC Device (Mgmt. Addr.): 192.168.101.10 Status: UP Device Alarm Summary: 0/0/0/0
Voice Endpoint: rgvoip-0-d-da-0-2-d9.lab.telesyn.corp
Voice Endpoint Port: TEL1 IG-CRV: gr303 (gr303)-1 Line Status: Unlock-Enabled

Alerts

Status	Failure Object	Alarm Message	Date/Time ▼

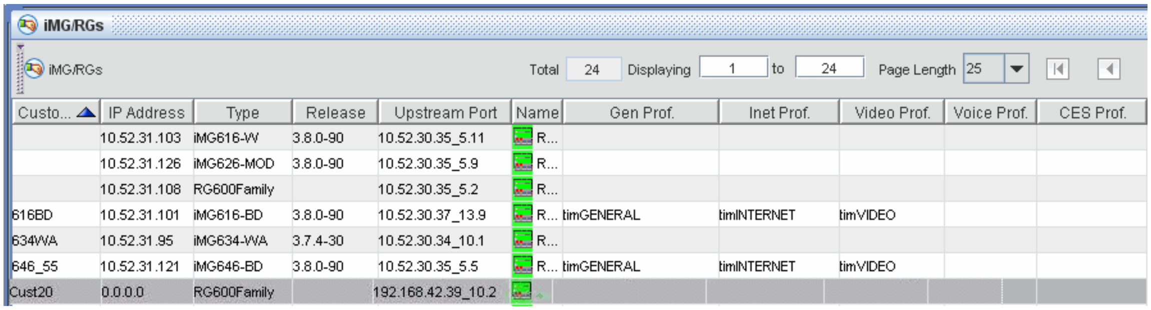
Fri Dec 02 15:20:47 EST 2005 - Polling of 192.168.42.39 successful.

FIGURE 21-50 Service Management Form - iMAP Port Configured, no iMG/RG Configured

Note the following:

- The Video/Data Port Configuration Panel includes the upstream port and card/port status
- The Voice Configuration Panel includes the Voice Endpoint (needed for DNS lookup for DHCP) and the Voice Endpoint Port (TEL1, which is the port the customer will plug the phone into).
- The Alerts Panel has any alarms. There should be no alarms.

14. Review the iMG/RG table, as shown in Figure 21-51.



Custo... ▲	IP Address	Type	Release	Upstream Port	Name	Gen Prof.	Inet Prof.	Video Prof.	Voice Prof.	CES Prof.
	10.52.31.103	iMG616-W	3.8.0-90	10.52.30.35_5.11	R...					
	10.52.31.126	iMG626-MOD	3.8.0-90	10.52.30.35_5.9	R...					
	10.52.31.108	RG600Family		10.52.30.35_5.2	R...					
616BD	10.52.31.101	iMG616-BD	3.8.0-90	10.52.30.37_13.9	R...	timGENERAL	timINTERNET	timVIDEO		
634WA	10.52.31.95	iMG634-WA	3.7.4-30	10.52.30.34_10.1	R...					
646_55	10.52.31.121	iMG646-BD	3.8.0-90	10.52.30.35_5.5	R...	timGENERAL	timINTERNET	timVIDEO		
Cust20	0.0.0.0	RG600Family		192.168.42.39_10.2						

FIGURE 21-51 IMG/RG Table - iMAP Port Configured, no iMG/RG Configured

Note the following:

- The Customer ID, Type (Family level), and Upstream Port are identified.
- The iMG/RG IP address, software release, and associated profiles are not included. These are filled in as a result of plugging in the iMG/RG by the customer, which begins the DHCP configuration steps.

21.15.3.4 Install the iMG/RG and Apply Power

Note: *Installation instructions are included with the iMG/RG packaging, and these should be read before continuing with this part of the Procedure, since these instructions will include detailed pictures, a listing of cables that are used for the interface connections, and any updates to product information.*

Note: *If a technician is installing the Ethernet version of the iMG/RG, a PC (laptop) can be connected directly to monitor the progress of the iMG/RG configuration (mainly the successful allocation of addresses by DHCP). The console cable is sold separately by ATI. Use n-8-1-38400 for the console port setting.*

For this part of the procedure, do the following:

1. Ensure the connection to the customer from the iMAP connection is active.
2. Remove the iMG/RG from its packaging.
3. Connect the WAN cable to the external interface port.
4. Apply power to the iMG/RG (usually by connecting the power cable to iMG/RG and then plugging it in).
5. Note the sequence of events that shows the iMG/RG as run through its initial and reboot sequence (for details refer to Detailed steps for DHCP Discovery).

21.15.3.5 Connect Devices and wait for Services to Begin

1. Note which ports are being used:

- LAN1 to a STB for video service
- LAN2 to a PC for internet service
- LAN3 - Unused
- TEL1 - to a telephone for voice service
- TEL2 - Unused

2. Connect the devices to the iMG/RG using the appropriate cables.
3. Once connected, devices will use DHCP and the provisioned components. When finished, all devices should be providing service. Test all devices to ensure they deliver the promised service(s).

21.15.4 Provisioning / De-Provisioning Voice Service

When a customer has video and data service (double-play), and wishes to add voice service, the use of AlliedView NMS makes this possible, through the use of profiles, with a small number of steps. Moreover, adding or removing a second line for a service is accomplished using only a few GUI screens. Finally, removing the voice service and going (back) to double play involves (re)applying the profile for double-play.

21.15.4.1 Add Voice Service (Double-play to Triple-Play)

1. Ensure prerequisites are met:

- Customer uses iMG/RG General Profile that enables double-play and has internet and video profiles

  - RG General - **DeskLab-1 Video-1 Data**

  - Internet - **HomeNetworkInet**

  - Video - **Video-Proxy**

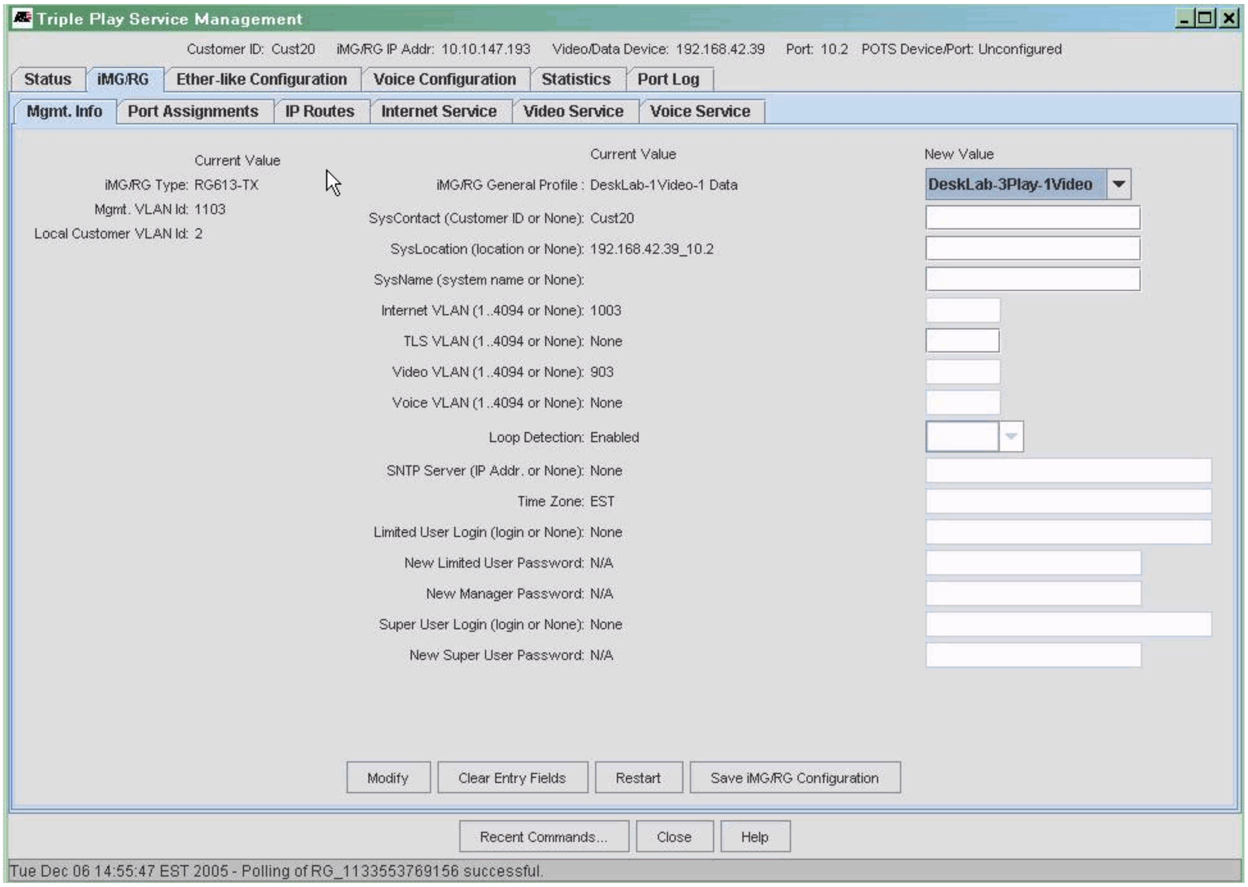
- There is an RG General Profile for Triple-Play that matches the customer attributes for double-play and adds the necessary attributes for voice (especially the voice VLAN and routes.

  - RG General - **DeskLab-3Play-1Video**

2. Find the iMG/RG for the customer in the iMG/RGs table using various methods:

- Bring up the iMG/RGs node in the Network Inventory table and do a search (Ctrl-F) on the Customer ID.
- Bring up the Ports node in the Network Inventory table and do a search (Ctrl-F) on the Customer ID.

3. Right click on the iMG/RG or Port and select **View/Modify Details**. This brings up the Triple Play Service Management screen.
4. Select the iMG/RG tab, which automatically shows the Mgmt. Info tab.
5. In the RG General profile pull-down, select the Profile DeskLab-3Play-1Video, as shown in Figure 21-52.



Customer ID: Cust20 iMG/RG IP Addr: 10.10.147.193 Video/Data Device: 192.168.42.39 Port: 10.2 POTS Device/Port: Unconfigured

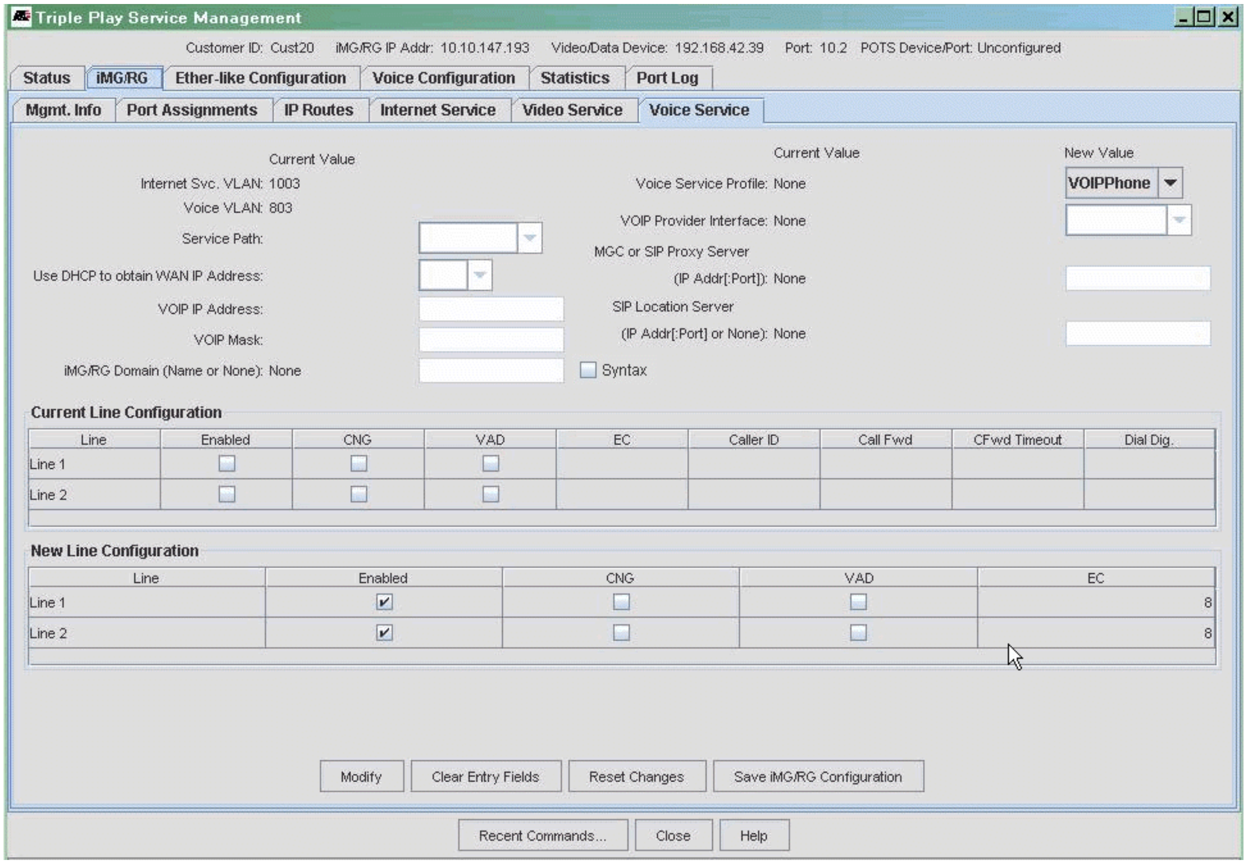
iMG/RG Type: RG613-TX
Mgmt. VLAN Id: 1103
Local Customer VLAN Id: 2

iMG/RG General Profile : DeskLab-1Video-1 Data — New Value: DeskLab-3Play-1Video
SysContact (Customer ID or None): Cust20
SysLocation (location or None): 192.168.42.39_10.2
SysName (system name or None):
Internet VLAN (1..4094 or None): 1003
TLS VLAN (1..4094 or None): None
Video VLAN (1..4094 or None): 903
Voice VLAN (1..4094 or None): None
Loop Detection: Enabled
SNTP Server (IP Addr. or None): None
Time Zone: EST
Limited User Login (login or None): None
New Limited User Password: N/A
New Manager Password: N/A
Super User Login (login or None): None
New Super User Password: N/A

Tue Dec 06 14:55:47 EST 2005 - Polling of RG_1133553769156 successful.

FIGURE 21-52 Applying Different RG General Profile for Triple-Play

6. Click **Modify**.
7. Note the results - The VLAN defined in the General Profile is added.
8. Still in the Mgmt. Info tab, select the Voice Service tab
9. For the Voice Service Profile pull-down, select VOIPPhone. Refer to Figure 21-53.



Customer ID: Cust20 iMG/RG IP Addr: 10.10.147.193 Video/Data Device: 192.168.42.39 Port: 10.2 POTS Device/Port: Unconfigured

	Current Value
Internet Svc. VLAN:	1003
Voice VLAN:	803
Service Path:	
Use DHCP to obtain WAN IP Address:	
VOIP IP Address:	
VOIP Mask:	
iMG/RG Domain (Name or None):	None

	Current Value	New Value
Voice Service Profile:	None	VOIPPhone
VOIP Provider Interface:	None	
MGC or SIP Proxy Server (IP Addr[:Port]):	None	
SIP Location Server (IP Addr[:Port] or None):	None	

□ Syntax

Current Line Configuration

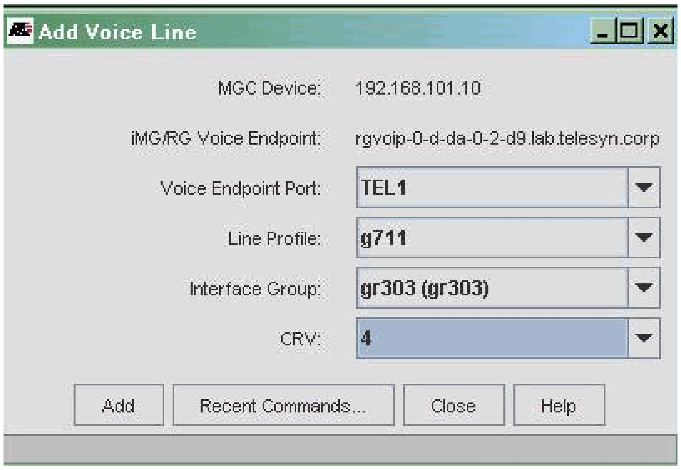
Line	Enabled	CNG	VAD	EC	Caller ID	Call Fwd	CFwd Timeout	Dial Dig.
Line 1	□	□	□					
Line 2	□	□	□					

New Line Configuration

Line	Enabled	CNG	VAD	EC
Line 1	☑	□	□	8
Line 2	☑	□	□	8

FIGURE 21-53 Applying Voice Profile

10. Click **Modify**.
11. Select the Status tab (there are no sub-tabs).
12. Click on Add Voice Line. The **Add Voice Line** form appears.
13. In the Add Voice Line form, note that the Voice Endpoint (used for DNS) is already defined, as well as the interface group. These were defined in the Voice service profile.
14. Select from the pull-down the Voice Endpoint Port, the Line Profile, and the CRV. Refer to Figure 21-54.



MGC Device:	192.168.101.10
iMG/RG Voice Endpoint:	rgvoip-0-d-da-0-2-d9.lab.telesyn.corp
Voice Endpoint Port:	TEL1
Line Profile:	g711
Interface Group:	gr303 (gr303)
CRV:	4

FIGURE 21-54 Add Voice Line (line 1)

15. Click **Add**.
16. Back on the Status tab, click on Update Customer Info.
17. Note the results.

Note: *For the Open Access Model, the same procedure would be used, with the administrator ensuring that there was no conflict in VLAN configuration between the iMG/RG General Profile and the Voice Service Profile.*

21.15.4.2 Add Second Voice Line

1. Ensure the prerequisites are met:

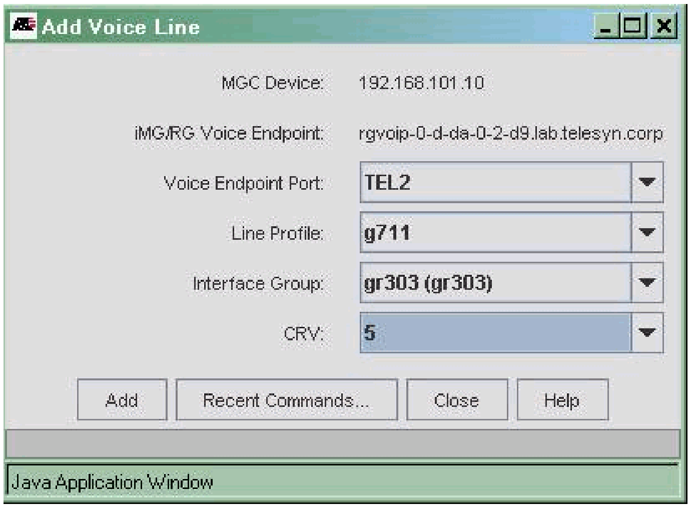
- The Voice Profile already supports more than one voice line.

2. Find the iMG/RG for the customer in the iMG/RGs table using various methods:

- Bring up the iMG/RGs node in the Network Inventory table and do a search (Ctrl-F) on the Customer ID.
- Bring up the Ports node in the Network Inventory table and do a search (Ctrl-F) on the Customer ID.

3. Right click on the iMG/RG or Port and select **View/Modify Details**. This brings up the Triple Play Service Management screen.
4. The Select tab should appear by default.
5. Click on **Add Voice Line**. The **Add Voice Line** form appears.
6. In the Add Voice Line form, note that the Voice Endpoint (used for DNS) is already defined, as well as the interface group. These were defined in the Voice service profile.
7. Select from the pull-down the Voice Endpoint Port, the Line Profile, and the CRV. Refer to Figure 21-55.

Note: *Since this is a second voice line, choose TEL2 for the Voice Endpoint Port; otherwise any new values chosen here will change the already existing voice endpoint.*



Add Voice Line

MGC Device: 192.168.101.10

iMG/RG Voice Endpoint: rgvoip-0-d-da-0-2-d9.lab.telesyn.corp

Voice Endpoint Port: TEL2

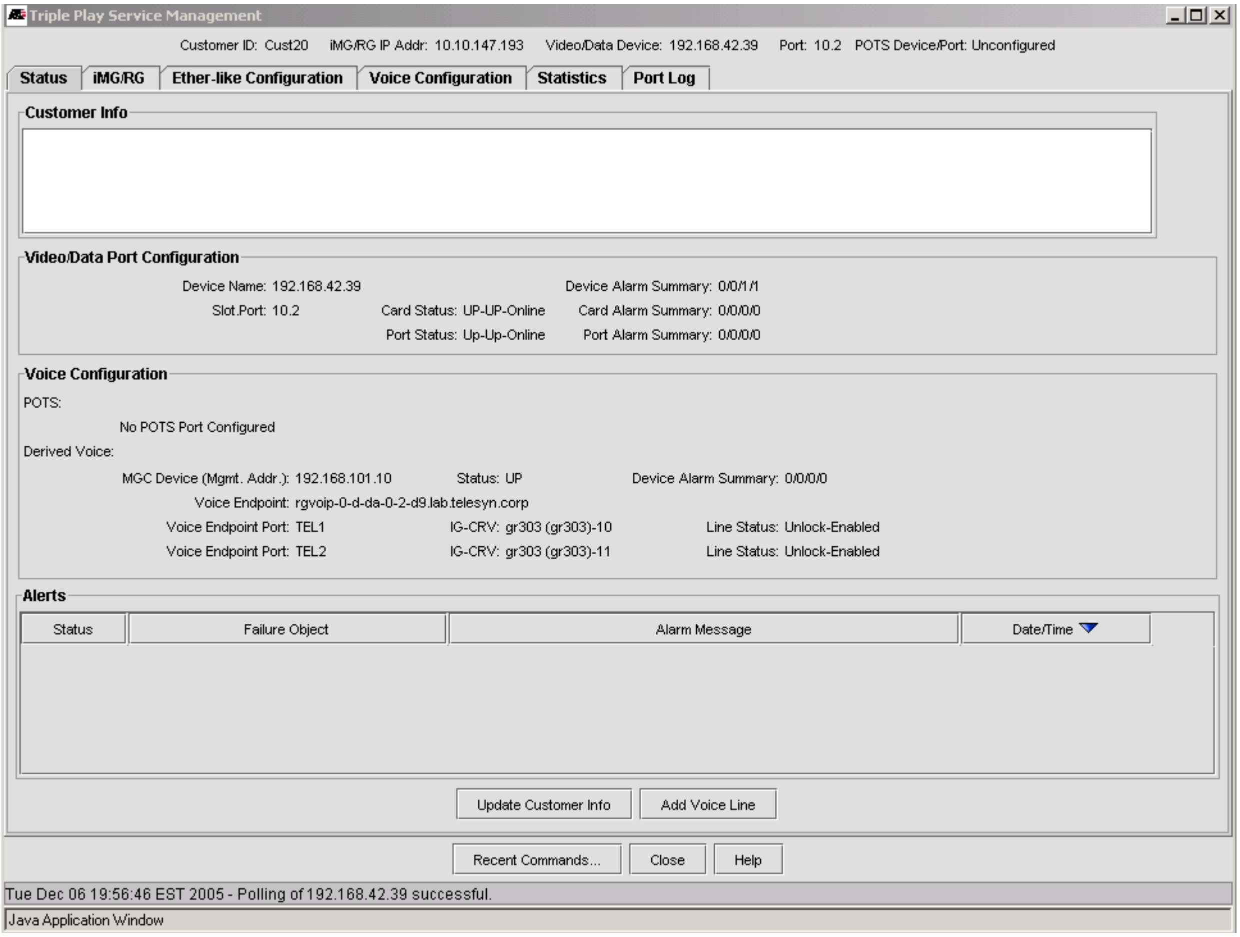
Line Profile: g711

Interface Group: gr303 (gr303)

CRV: 5

FIGURE 21-55 Add Voice Line (line 2)

8. Click on the now activated **Add**.
9. Back on the Status tab, click on **Update Customer Info**.
10. Note the results. Refer to Figure 21-56.



Customer ID: Cust20 iMG/RG IP Addr: 10.10.147.193 Video/Data Device: 192.168.42.39 Port: 10.2 POTS Device/Port: Unconfigured

Device Name: 192.168.42.39 Device Alarm Summary: 0/0/1/1
Slot.Port: 10.2 Card Status: UP-UP-Online Card Alarm Summary: 0/0/0/0
Port Status: Up-Up-Online Port Alarm Summary: 0/0/0/0

POTS:
No POTS Port Configured
Derived Voice:
MGC Device (Mgmt. Addr.): 192.168.101.10 Status: UP Device Alarm Summary: 0/0/0/0
Voice Endpoint: rgvoip-0-d-da-0-2-d9.lab.telesyn.corp
Voice Endpoint Port: TEL1 IG-CRV: gr303 (gr303)-10 Line Status: Unlock-Enabled
Voice Endpoint Port: TEL2 IG-CRV: gr303 (gr303)-11 Line Status: Unlock-Enabled

Tue Dec 06 19:56:46 EST 2005 - Polling of 192.168.42.39 successful.

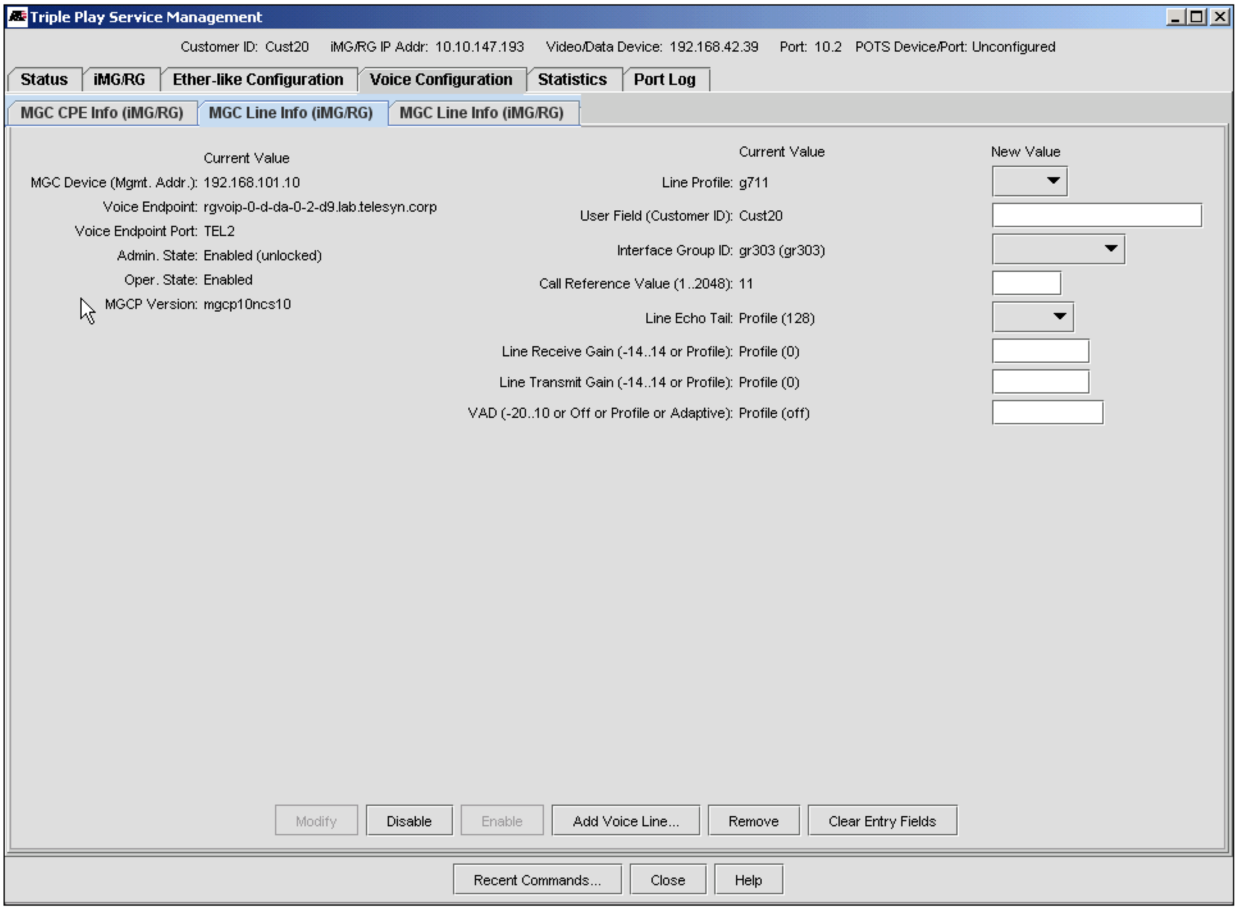
FIGURE 21-56 Results of Second Voice Line Added

21.15.4.3 Remove Second Voice Line

1. Find the iMG/RG for the customer in the iMG/RGs table using various methods:

- Bring up the iMG/RGs node in the Network Inventory table and do a search (Ctrl-F) on the Customer ID.
- Bring up the Ports node in the Network Inventory table and do a search (Ctrl-F) on the Customer ID.

2. Right click on the iMG/RG or Port and select **View/Modify Details**. This brings up the Triple Play Service Management screen.
3. The Select tab should appear by default.
4. Select the Voice Configuration tab. Two MGC Info subtabs should appear, one for each voice line. Refer to Figure 21-57.



Customer ID: Cust20 iMG/RG IP Addr: 10.10.147.193 Video/Data Device: 192.168.42.39 Port: 10.2 POTS Device/Port: Unconfigured

	Current Value
MGC Device (Mgmt. Addr.):	192.168.101.10
Voice Endpoint:	rgvoip-0-d-da-0-2-d9.lab.telesyn.corp
Voice Endpoint Port:	TEL2
Admin. State:	Enabled (unlocked)
Oper. State:	Enabled
MGCP Version:	mgcp10ncs10

	Current Value	New Value
Line Profile:	g711	
User Field (Customer ID):	Cust20	
Interface Group ID:	gr303 (gr303)	
Call Reference Value (1..2048):	11	
Line Echo Tail:	Profile (128)	
Line Receive Gain (-14..14 or Profile):	Profile (0)	
Line Transmit Gain (-14..14 or Profile):	Profile (0)	
VAD (-20..10 or Off or Profile or Adaptive):	Profile (off)	

FIGURE 21-57 Two MGC Tabs (one for each Voice Line)

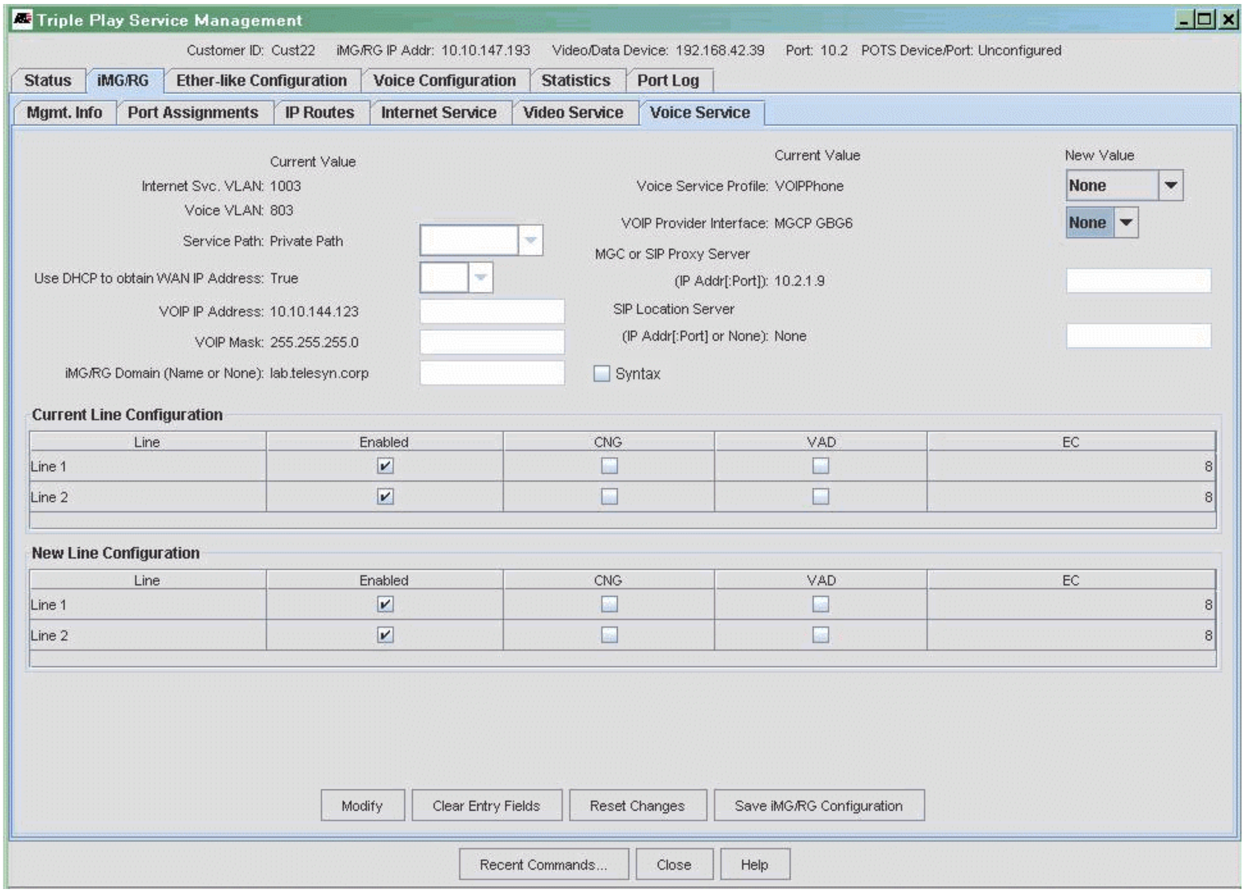
5. Click **Remove.**
6. When the Confirmation window appears, click on Yes.
7. Note the results. The MGC tab is removed and only one MGC tab remains.

21.15.4.4 Remove Voice Service (Triple- to Double-Play)

1. Ensure the pre-requisites are met:

- General Profile available to support the result of customer having no voice service (double play)

2. Right click on the iMG/RG or Port and select **View/Modify Details**. This brings up the Triple Play Service Management screen.
3. Select the iMG/RG - Voice Service tab.
4. For the Voice Service Profile and VOIP Provider Interface, select None, as shown in the following figure.



Customer ID: Cust22 iMG/RG IP Addr: 10.10.147.193 Video/Data Device: 192.168.42.39 Port: 10.2 POTS Device/Port: Unconfigured

Current Value

Internet Svc. VLAN: 1003

Voice VLAN: 803

Service Path: Private Path

Use DHCP to obtain WAN IP Address: True

VOIP IP Address: 10.10.144.123

VOIP Mask: 255.255.255.0

iMG/RG Domain (Name or None): lab.telesyn.corp

	Current Value	New Value
Voice Service Profile:	VOIPPhone	None
VOIP Provider Interface:	MGCP GBG6	None
MGC or SIP Proxy Server (IP Addr[:Port]):	10.2.1.9	
SIP Location Server (IP Addr[:Port] or None):	None	

□ Syntax

Current Line Configuration

Line	Enabled	CNG	VAD	EC
Line 1	☑	□	□	8
Line 2	☑	□	□	8

New Line Configuration

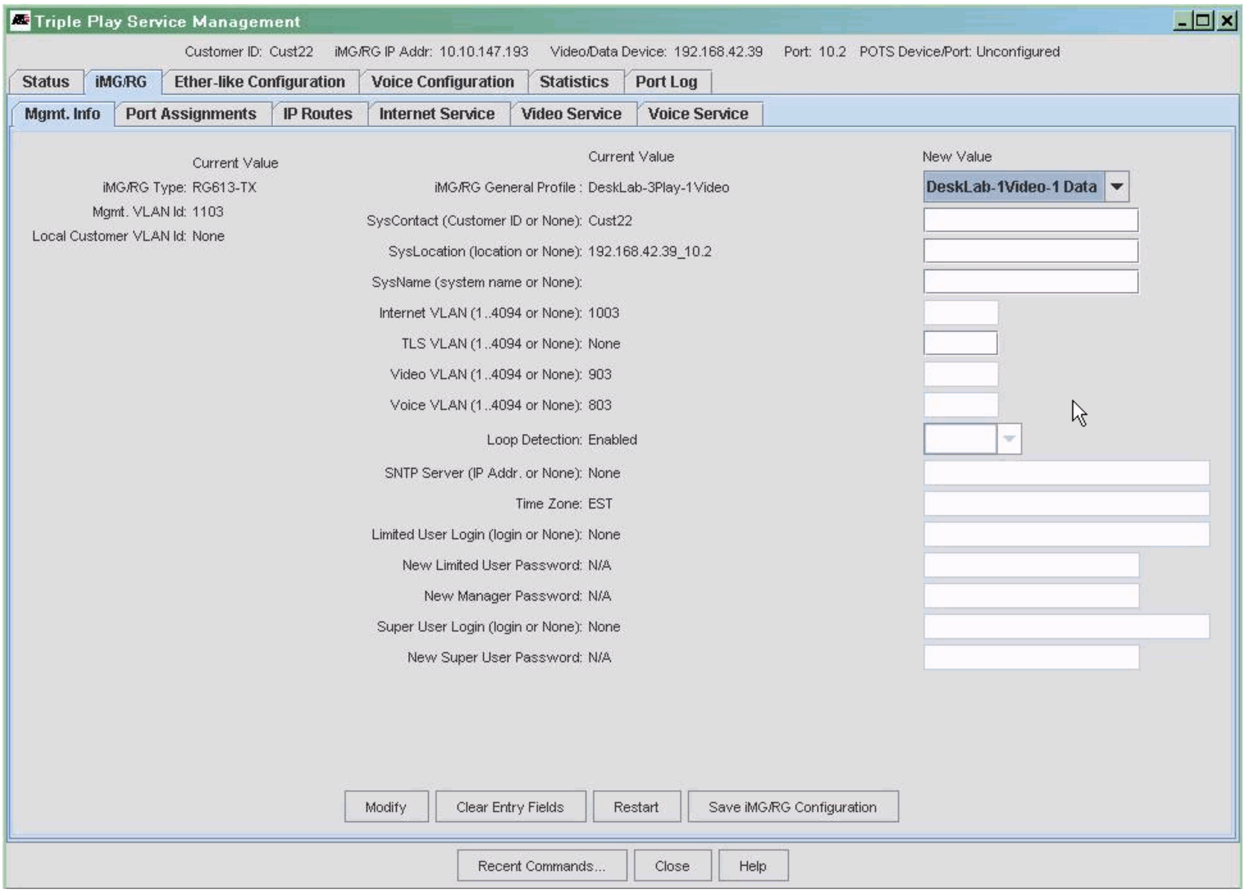
Line	Enabled	CNG	VAD	EC
Line 1	☑	□	□	8
Line 2	☑	□	□	8

FIGURE 21-58 Deleting Voice Profile

5. Click **Modify**.

Note: At this point you could select Save iMG/RG Configuration, and the customer would have no voice service but still have it configured on the RG.

6. Select the Mgmt. Info tab (still under the iMG/RG tab).
7. For the RG General Profile, select the double-play General Profile the customer will use. Refer to the following figure.



Customer ID: Cust22 iMG/RG IP Addr: 10.10.147.193 Video/Data Device: 192.168.42.39 Port: 10.2 POTS Device/Port: Unconfigured

Current Value
iMG/RG Type: RG613-TX
Mgmt. VLAN Id: 1103
Local Customer VLAN Id: None

	Current Value	New Value
iMG/RG General Profile :	DeskLab-3Play-1Video	DeskLab-1Video-1 Data
SysContact (Customer ID or None):	Cust22	
SysLocation (location or None):	192.168.42.39_10.2	
SysName (system name or None):		
Internet VLAN (1..4094 or None):	1003	
TLS VLAN (1..4094 or None):	None	
Video VLAN (1..4094 or None):	903	
Voice VLAN (1..4094 or None):	803	
Loop Detection:	Enabled	
SNTP Server (IP Addr. or None):	None	
Time Zone:	EST	
Limited User Login (login or None):	None	
New Limited User Password:	N/A	
New Manager Password:	N/A	
Super User Login (login or None):	None	
New Super User Password:	N/A	

FIGURE 21-59 Customer Using Profile for Double Play (no Voice)

8. Select **Save iMG/RG Configuration**.
9. As the changes takes effect, any phone connected to the RG will no longer have dial tone.

21.15.5 Provisioning / De-Provisioning Video Service

When a customer has voice and data service (double-play), and wishes to add video service, the use of AlliedView NMS makes this possible, through the use of profiles, with a small number of steps. Moreover, adding or removing a second line for a service is accomplished using only a few GUI screens. Finally, removing the voice service and going (back) to double play involves (re)applying the profile for double-play.

21.15.5.1 Add Video Service (Double-play to Triple-Play)

1. Ensure prerequisites are met:

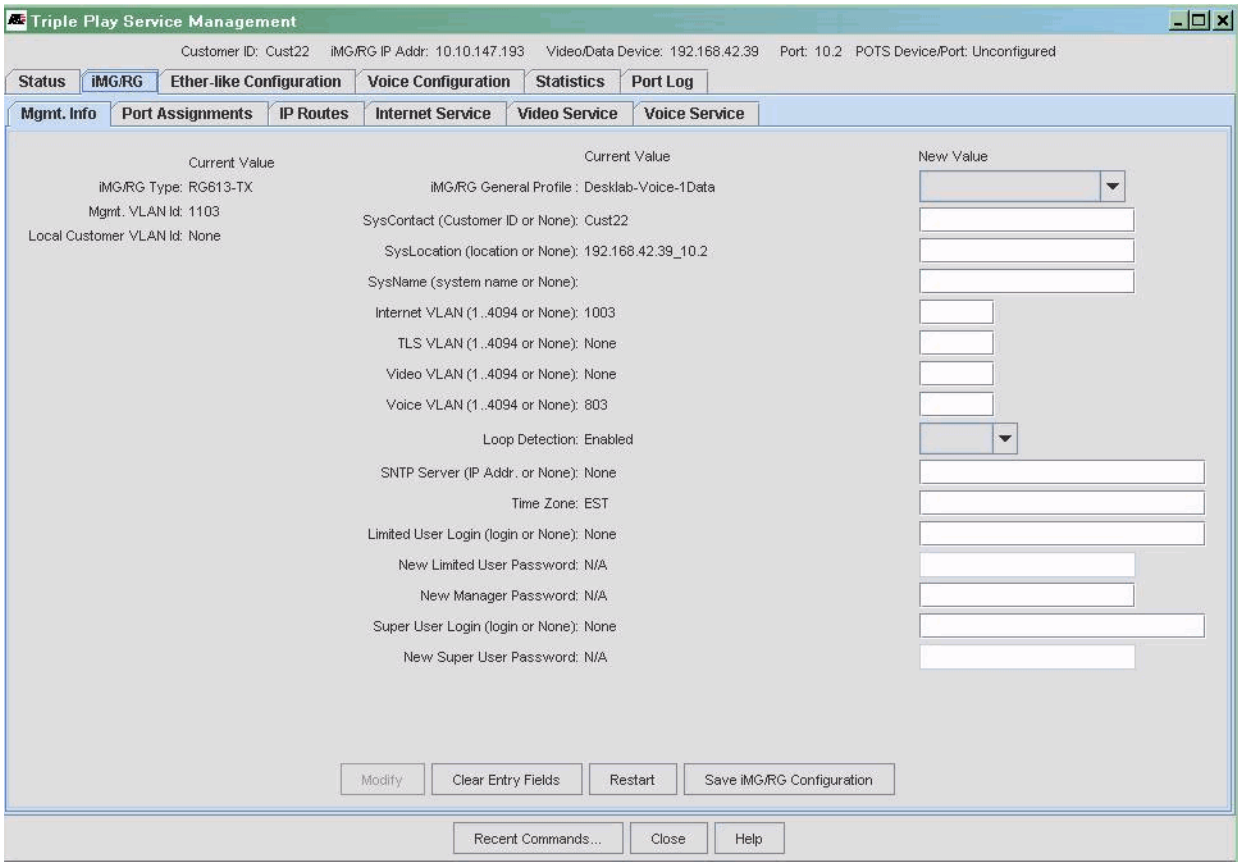
- Customer uses RG General Profile that enables double-play and has internet and voice profiles

  - RG General - **DeskLab-Voice-1 Data**

  - Internet - **HomeNetworkInet**

  - Voice - **VOIPPhone**

  Figure 21-60 shows this configuration. Note the name of the General Profile and that there is no video VLAN.



Customer ID: Cust22 iMG/RG IP Addr: 10.10.147.193 Video/Data Device: 192.168.42.39 Port: 10.2 POTS Device/Port: Unconfigured

	Current Value
iMG/RG Type:	RG613-TX
Mgmt. VLAN Id:	1103
Local Customer VLAN Id:	None

	Current Value	New Value
iMG/RG General Profile :	Desklab-Voice-1Data	
SysContact (Customer ID or None):	Cust22	
SysLocation (location or None):	192.168.42.39_10.2	
SysName (system name or None):		
Internet VLAN (1..4094 or None):	1003	
TLS VLAN (1..4094 or None):	None	
Video VLAN (1..4094 or None):	None	
Voice VLAN (1..4094 or None):	803	
Loop Detection:	Enabled	
SNTP Server (IP Addr. or None):	None	
Time Zone:	EST	
Limited User Login (login or None):	None	
New Limited User Password:	N/A	
New Manager Password:	N/A	
Super User Login (login or None):	None	
New Super User Password:	N/A	

FIGURE 21-60 Customer without Video (Double Play)

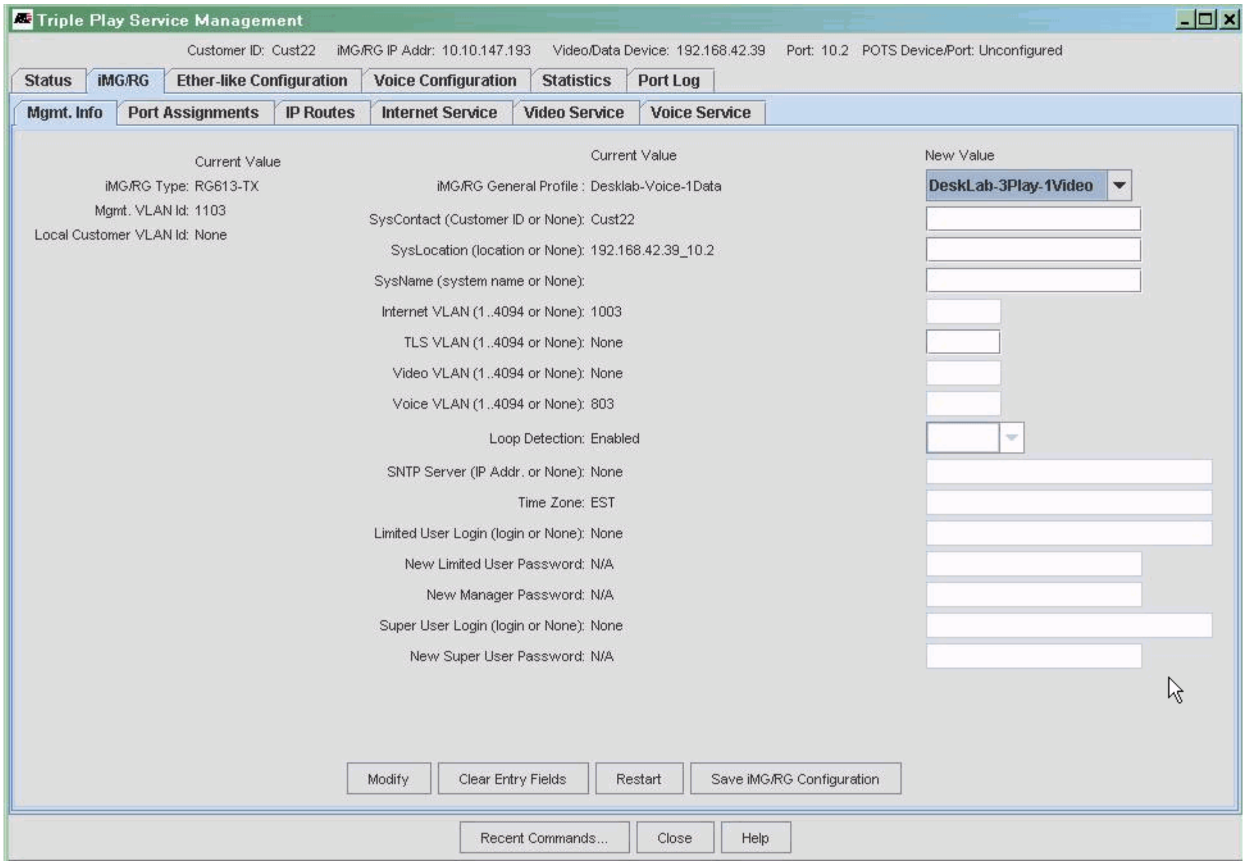
- There is an RG General Profile for Triple-Play that matches the customer attributes for double-play and adds the necessary attributes for video (especially the video VLAN and routes).

  - RG General - **DeskLab-3Play-1Video**

2. Find the iMG/RG for the customer in the iMG/RGs table using various methods:

- Bring up the iMG/RGs node in the Network Inventory table and do a search (Ctrl-F) on the Customer ID.
- Bring up the Ports node in the Network Inventory table and do a search (Ctrl-F) on the Customer ID.

3. Right click on the iMG/RG or Port and select **View/Modify Details**. This brings up the Triple Play Service Management screen.
4. Select the iMG/RG tab, which automatically shows the Mgmt. Info tab.
5. In the RG General profile pull-down, select the Profile **DeskLab-3Play-1Video**, as shown in Figure 21-61.



Customer ID: Cust22 iMG/RG IP Addr: 10.10.147.193 Video/Data Device: 192.168.42.39 Port: 10.2 POTS Device/Port: Unconfigured

Current Value

iMG/RG Type: RG613-TX

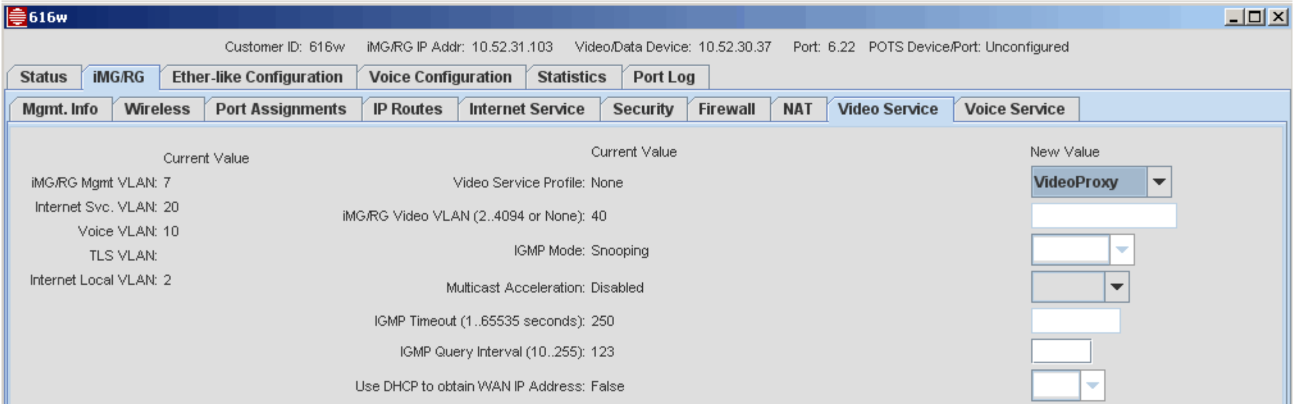
Mgmt. VLAN Id: 1103

Local Customer VLAN Id: None

	Current Value	New Value
iMG/RG General Profile :	Desklab-Voice-1Data	DeskLab-3Play-1Video
SysContact (Customer ID or None):	Cust22	
SysLocation (location or None):	192.168.42.39_10.2	
SysName (system name or None):		
Internet VLAN (1..4094 or None):	1003	
TLS VLAN (1..4094 or None):	None	
Video VLAN (1..4094 or None):	None	
Voice VLAN (1..4094 or None):	803	
Loop Detection:	Enabled	
SNTP Server (IP Addr. or None):	None	
Time Zone:	EST	
Limited User Login (login or None):	None	
New Limited User Password:	N/A	
New Manager Password:	N/A	
Super User Login (login or None):	None	
New Super User Password:	N/A	

FIGURE 21-61 Applying Different RG General Profile for Triple-Play

6. Click on **Modify**.
7. Note the results - There is now a VLAN provisioned for one video.
8. Still in the Mgmt. Info tab, select the Video Service tab.
9. For the Video Service Profile pull-down, select **Video-Proxy**. Refer to Figure 21-62.



Customer ID: 616w iMG/RG IP Addr: 10.52.31.103 Video/Data Device: 10.52.30.37 Port: 6.22 POTS Device/Port: Unconfigured

Current Value

iMG/RG Mgmt VLAN: 7

Internet Svc. VLAN: 20

Voice VLAN: 10

TLS VLAN:

Internet Local VLAN: 2

	Current Value	New Value
Video Service Profile:	None	VideoProxy
iMG/RG Video VLAN (2..4094 or None):	40	
IGMP Mode:	Snooping	
Multicast Acceleration:	Disabled	
IGMP Timeout (1..65535 seconds):	250	
IGMP Query Interval (10..255):	123	
Use DHCP to obtain WAN IP Address:	False	

FIGURE 21-62 Applying Video Profile

10. Click on the now active **Modify**.
11. Note the results - The Video Service Profile changes form None to Video-Proxy with the Video Svc. VLAN from the RG GeneralMgmt profile

Note: *Do not make changes to the IGMP values, or the video service will be out of synch with the video profile. (If you do so, and * will appear next to the Profile Name.)*

12. Return to the Mgmt. Info sub-tab.
13. Click on **Save iMG/RG Configuration**.
14. Back on the Status tab, click on **Update Customer Info**.
15. Note the results. Video should no longer be available.

Note: *For the Open Access Model, the same procedure would be used, with the administrator ensuring that there was no conflict in VLAN configuration between the iMG/RG General Profile and the Video Service Profile.*

21.15.5.2 Add Second Video Line

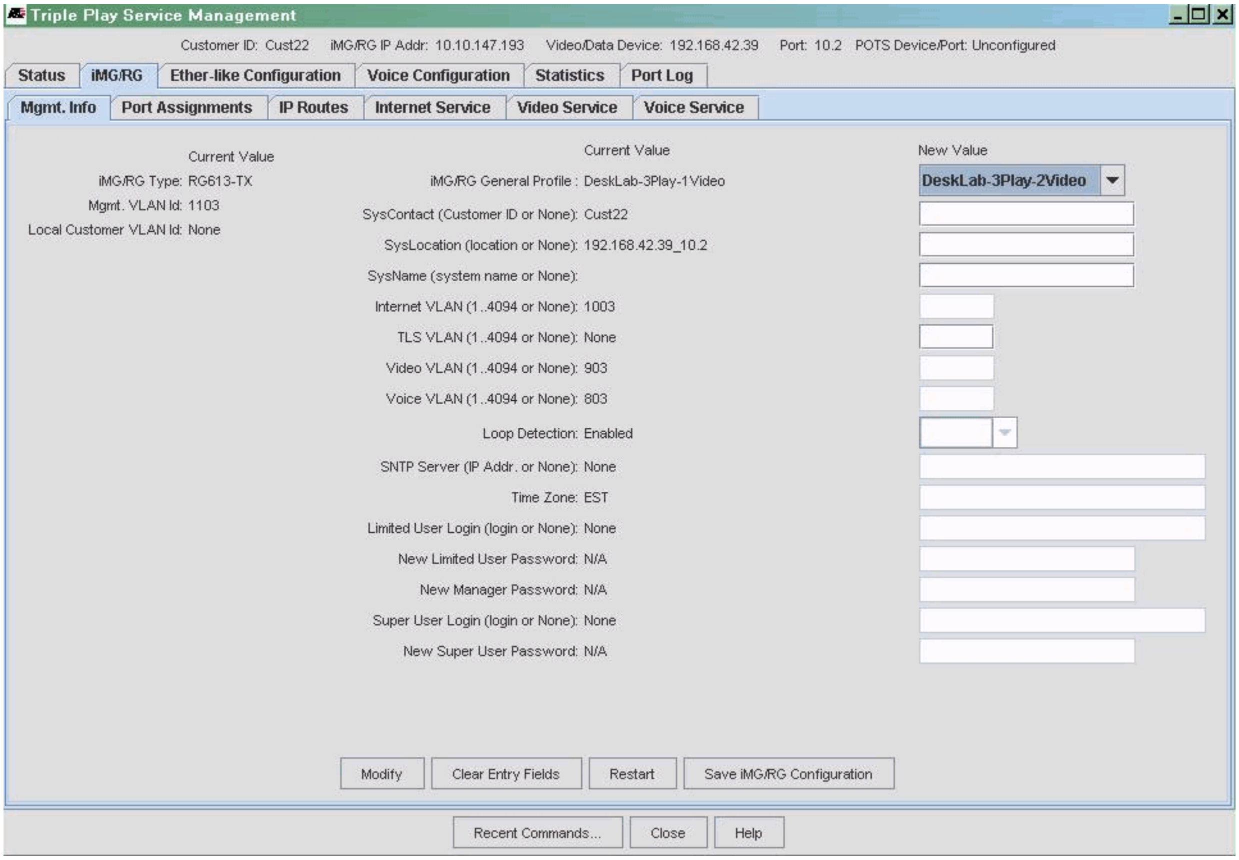
1. Ensure the prerequisites are met:

- An RG General Profile exists that supports more than one video, i.e. **DeskLab-3-play-2Video**.

2. Find the iMG/RG for the customer in the iMG/RGs table using various methods:

- Bring up the iMG/RGs node in the Network Inventory table and do a search (Ctrl-F) on the Customer ID.
- Bring up the Ports node in the Network Inventory table and do a search (Ctrl-F) on the Customer ID.

3. Right click on the iMG/RG or Port and select **View/Modify Details**. This brings up the Triple Play Service Management screen.
4. Select the iMG/RG tab, which automatically shows the Mgmt. Info tab.
5. In the RG General profile pull-down, select the Profile **DeskLab-3Play-2Video**, as shown in Figure 21-63.



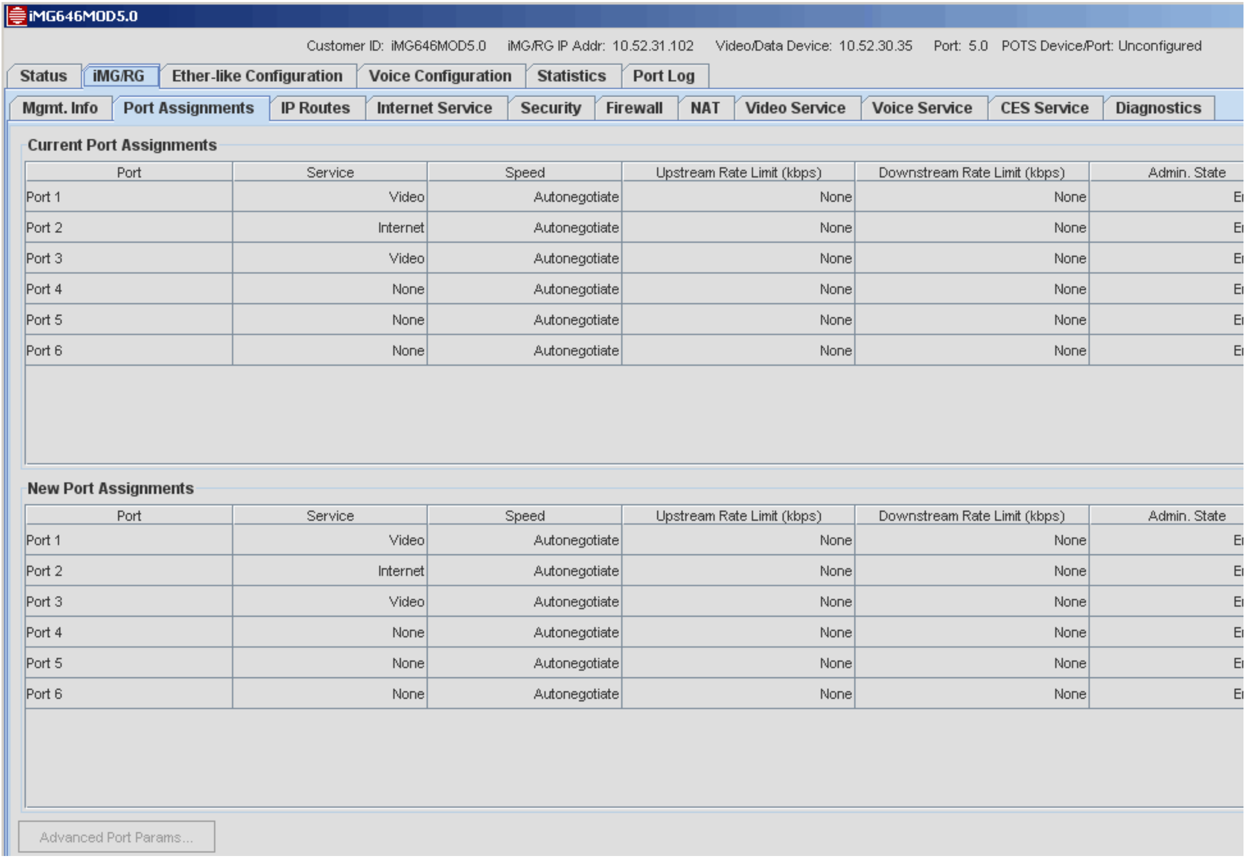
Customer ID: Cust22 iMG/RG IP Addr: 10.10.147.193 Video/Data Device: 192.168.42.39 Port: 10.2 POTS Device/Port: Unconfigured

Current Value
iMG/RG Type: RG613-TX
Mgmt. VLAN Id: 1103
Local Customer VLAN Id: None

Current Value		New Value
iMG/RG General Profile :	DeskLab-3Play-1Video	DeskLab-3Play-2Video
SysContact (Customer ID or None):	Cust22	
SysLocation (location or None):	192.168.42.39_10.2	
SysName (system name or None):		
Internet VLAN (1..4094 or None):	1003	
TLS VLAN (1..4094 or None):	None	
Video VLAN (1..4094 or None):	903	
Voice VLAN (1..4094 or None):	803	
Loop Detection:	Enabled	
SNTP Server (IP Addr. or None):	None	
Time Zone:	EST	
Limited User Login (login or None):	None	
New Limited User Password:	N/A	
New Manager Password:	N/A	
Super User Login (login or None):	None	
New Super User Password:	N/A	

FIGURE 21-63 Applying Different RG General Profile for Triple-Play (Second VIdeo)

6. Click **Modify**.
7. Click **Save iMG/RG Configuration**.
8. Back on the Status tab, click on **Update Customer Info**.
9. Note the results: On the iMG/RG Port Assignments tab, there are two ports for Video, 1 and 3, as shown in the following figure.
10. Restart cpe (iMG/RG).



Customer ID: iMG646MOD5.0 iMG/RG IP Addr: 10.52.31.102 Video/Data Device: 10.52.30.35 Port: 5.0 POTS Device/Port: Unconfigured

Current Port Assignments

Port	Service	Speed	Upstream Rate Limit (kbps)	Downstream Rate Limit (kbps)	Admin. State
Port 1	Video	Autonegotiate	None	None	E
Port 2	Internet	Autonegotiate	None	None	E
Port 3	Video	Autonegotiate	None	None	E
Port 4	None	Autonegotiate	None	None	E
Port 5	None	Autonegotiate	None	None	E
Port 6	None	Autonegotiate	None	None	E

New Port Assignments

Port	Service	Speed	Upstream Rate Limit (kbps)	Downstream Rate Limit (kbps)	Admin. State
Port 1	Video	Autonegotiate	None	None	E
Port 2	Internet	Autonegotiate	None	None	E
Port 3	Video	Autonegotiate	None	None	E
Port 4	None	Autonegotiate	None	None	E
Port 5	None	Autonegotiate	None	None	E
Port 6	None	Autonegotiate	None	None	E

FIGURE 21-64 Results of Second Video Line Added (Ports)

21.15.5.3 Remove Second Video Line

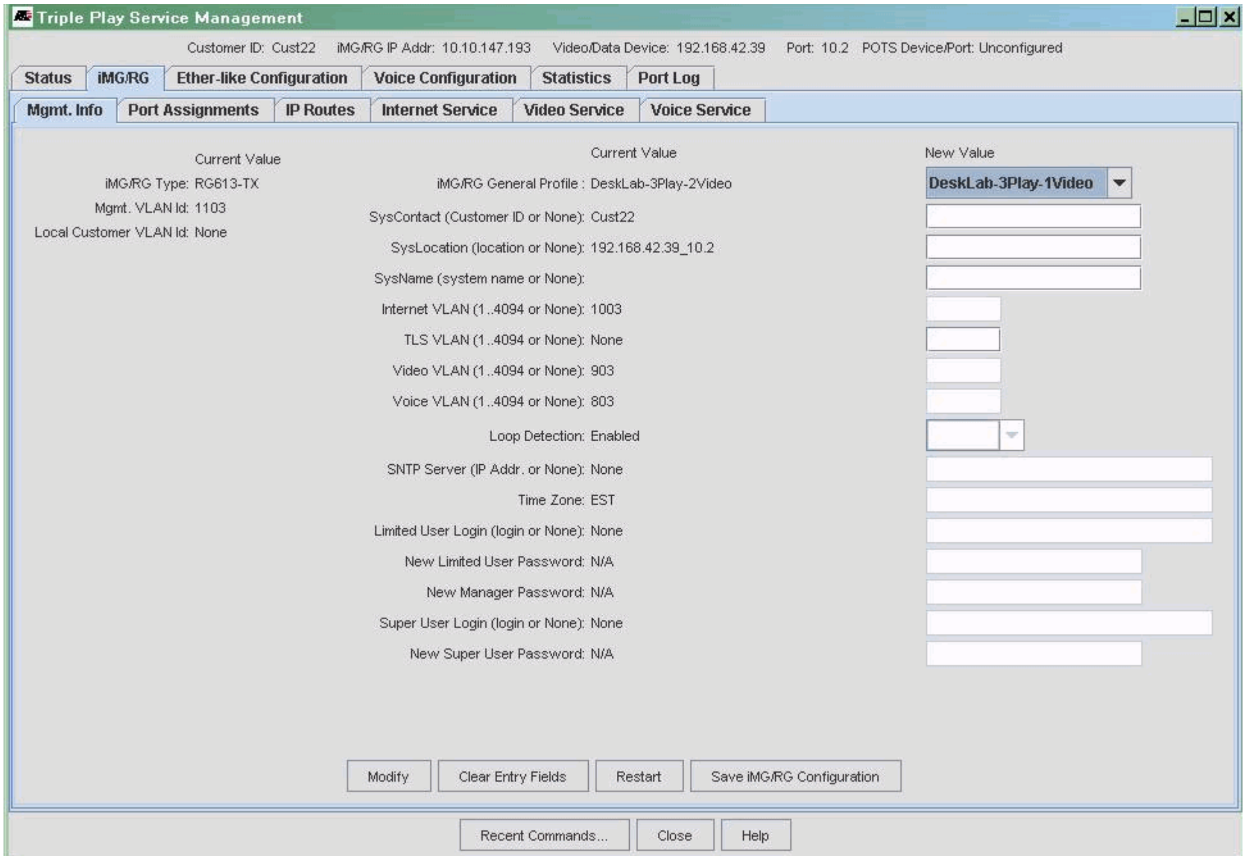
1. Ensure the prerequisites are met:

- An RG General Profile exists that supports more than one video, i.e. **DeskLab-3-play-1Video**.

2. Find the iMG/RG for the customer in the iMG/RGs table using various methods:

- Bring up the iMG/RGs node in the Network Inventory table and do a search (Ctrl-F) on the Customer ID.
- Bring up the Ports node in the Network Inventory table and do a search (Ctrl-F) on the Customer ID.

3. Right click on the iMG/RG or Port and select **View/Modify Details**. This brings up the Triple Play Service Management screen.
4. Select the iMG/RG tab, which automatically shows the Mgmt. Info tab.
5. In the RG General profile pull-down, select the Profile **DeskLab-3Play-1Video**, as shown in Figure 21-65.



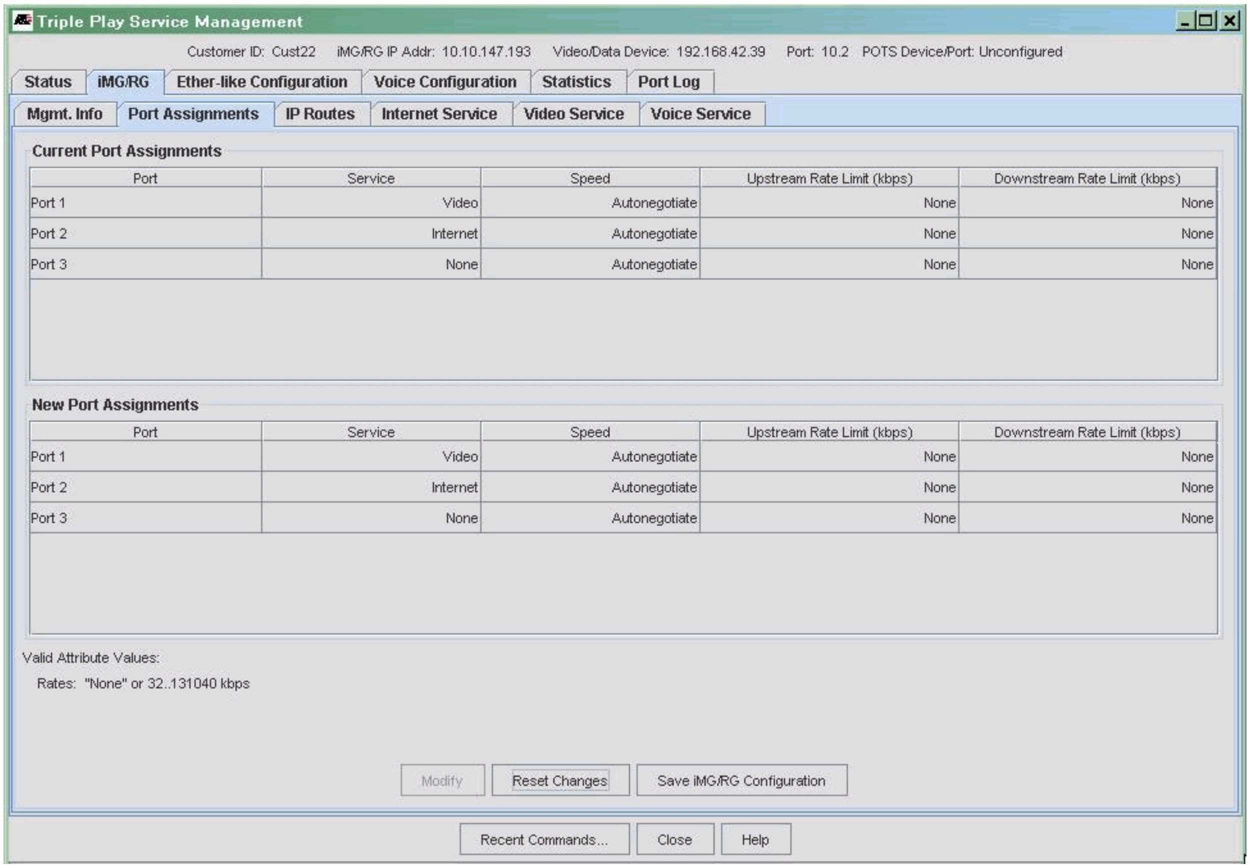
Customer ID: Cust22 iMG/RG IP Addr: 10.10.147.193 Video/Data Device: 192.168.42.39 Port: 10.2 POTS Device/Port: Unconfigured

	Current Value
iMG/RG Type:	RG613-TX
Mgmt. VLAN Id:	1103
Local Customer VLAN Id:	None

	Current Value	New Value
iMG/RG General Profile :	DeskLab-3Play-2Video	DeskLab-3Play-1Video
SysContact (Customer ID or None):	Cust22	
SysLocation (location or None):	192.168.42.39_10.2	
SysName (system name or None):		
Internet VLAN (1..4094 or None):	1003	
TLS VLAN (1..4094 or None):	None	
Video VLAN (1..4094 or None):	903	
Voice VLAN (1..4094 or None):	803	
Loop Detection:	Enabled	
SNTP Server (IP Addr. or None):	None	
Time Zone:	EST	
Limited User Login (login or None):	None	
New Limited User Password:	N/A	
New Manager Password:	N/A	
Super User Login (login or None):	None	
New Super User Password:	N/A	

FIGURE 21-65 Applying Different RG General Profile for Triple-Play (Remove Second VIdeo)

6. Click **Modify**.
7. Click on **Save iMG/RG Configuration**.
8. Back on the Status tab, click on **Update Customer Info**.
9. Note the results. In the Port Assignments tab, there is only one video port. Refer to the following figure.
10. At the iMG/RG/Mgmt. Info tab, select **Save iMG/RG Configuration**.
11. Restart the CPE (iMG/RG)


Triple Play Service Management
Customer ID: Cust22 iMG/RG IP Addr: 10.10.147.193 Video/Data Device: 192.168.42.39 Port: 10.2 POTS Device/Port: Unconfigured
Status
iMG/RG
Ether-like Configuration
Voice Configuration
Statistics
Port Log
Mgmt. Info
Port Assignments
IP Routes
Internet Service
Video Service
Voice Service

Current Port Assignments

Port	Service	Speed	Upstream Rate Limit (kbps)	Downstream Rate Limit (kbps)
Port 1	Video	Autonegotiate	None	None
Port 2	Internet	Autonegotiate	None	None
Port 3	None	Autonegotiate	None	None

New Port Assignments

Port	Service	Speed	Upstream Rate Limit (kbps)	Downstream Rate Limit (kbps)
Port 1	Video	Autonegotiate	None	None
Port 2	Internet	Autonegotiate	None	None
Port 3	None	Autonegotiate	None	None

Valid Attribute Values:
Rates: "None" or 32..131040 kbps

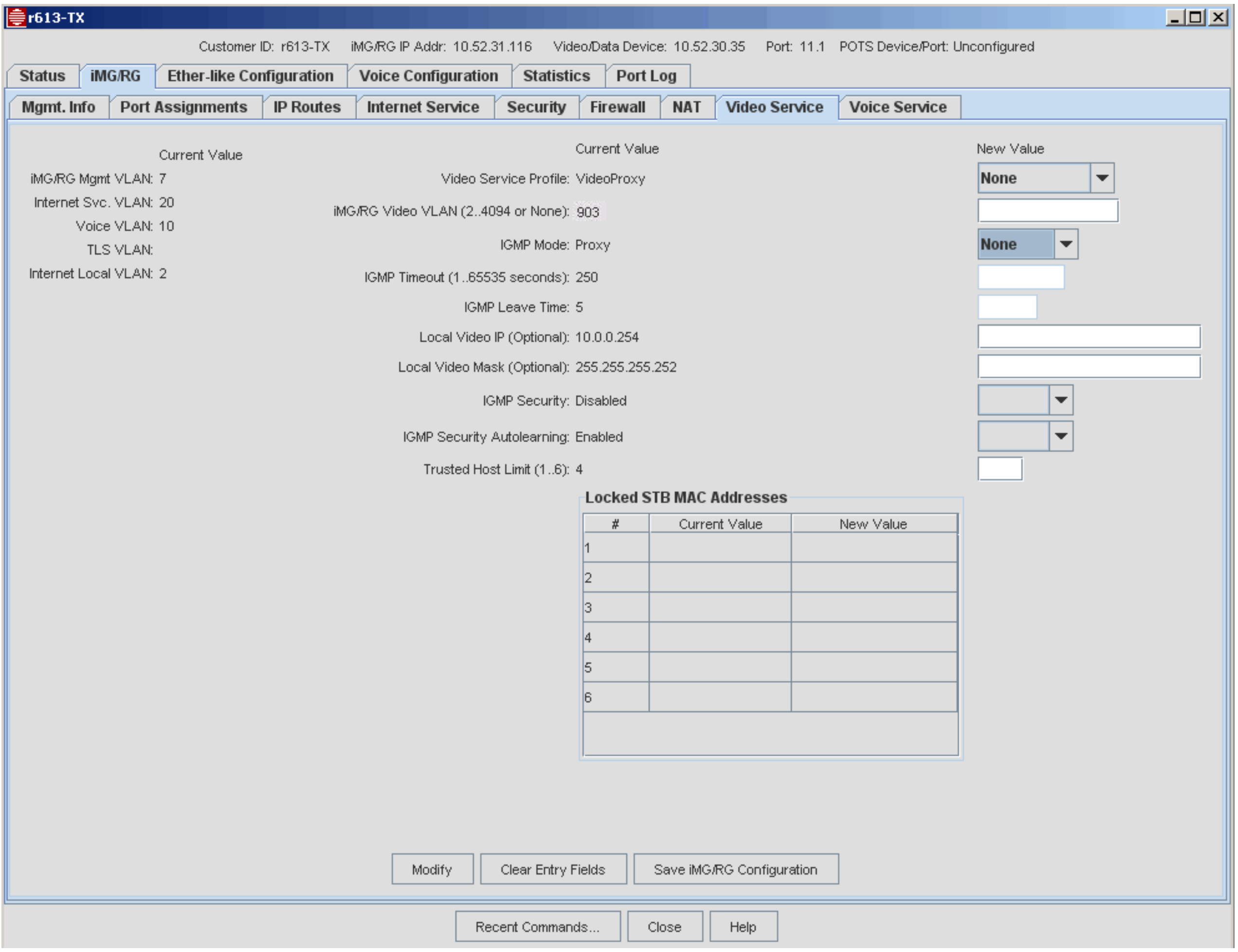
FIGURE 21-66 Results of Second Video Line Removed

21.15.5.4 Remove Video Service (Triple- to Double-Play)

1. Ensure the pre-requisites are met:

- General Profile available to support the result of customer having no video service (double play)

2. Right click on the iMG/RG or Port and select **View/Modify Details**. This brings up the Triple Play Service Management screen.
3. Select the iMG/RG - Video Service tab.
4. For the Video Service Profile and IGMP Mode, select **None**, as shown in the following figure.



Customer ID: r613-TX iMG/RG IP Addr: 10.52.31.116 Video/Data Device: 10.52.30.35 Port: 11.1 POTS Device/Port: Unconfigured

Current Value
iMG/RG Mgmt VLAN: 7
Internet Svc. VLAN: 20
Voice VLAN: 10
TLS VLAN:
Internet Local VLAN: 2

	Current Value	New Value
Video Service Profile:	VideoProxy	None
iMG/RG Video VLAN (2..4094 or None):	903	
IGMP Mode:	Proxy	None
IGMP Timeout (1..65535 seconds):	250	
IGMP Leave Time:	5	
Local Video IP (Optional):	10.0.0.254	
Local Video Mask (Optional):	255.255.255.252	
IGMP Security:	Disabled	
IGMP Security Autolearning:	Enabled	
Trusted Host Limit (1..6):	4	

Locked STB MAC Addresses

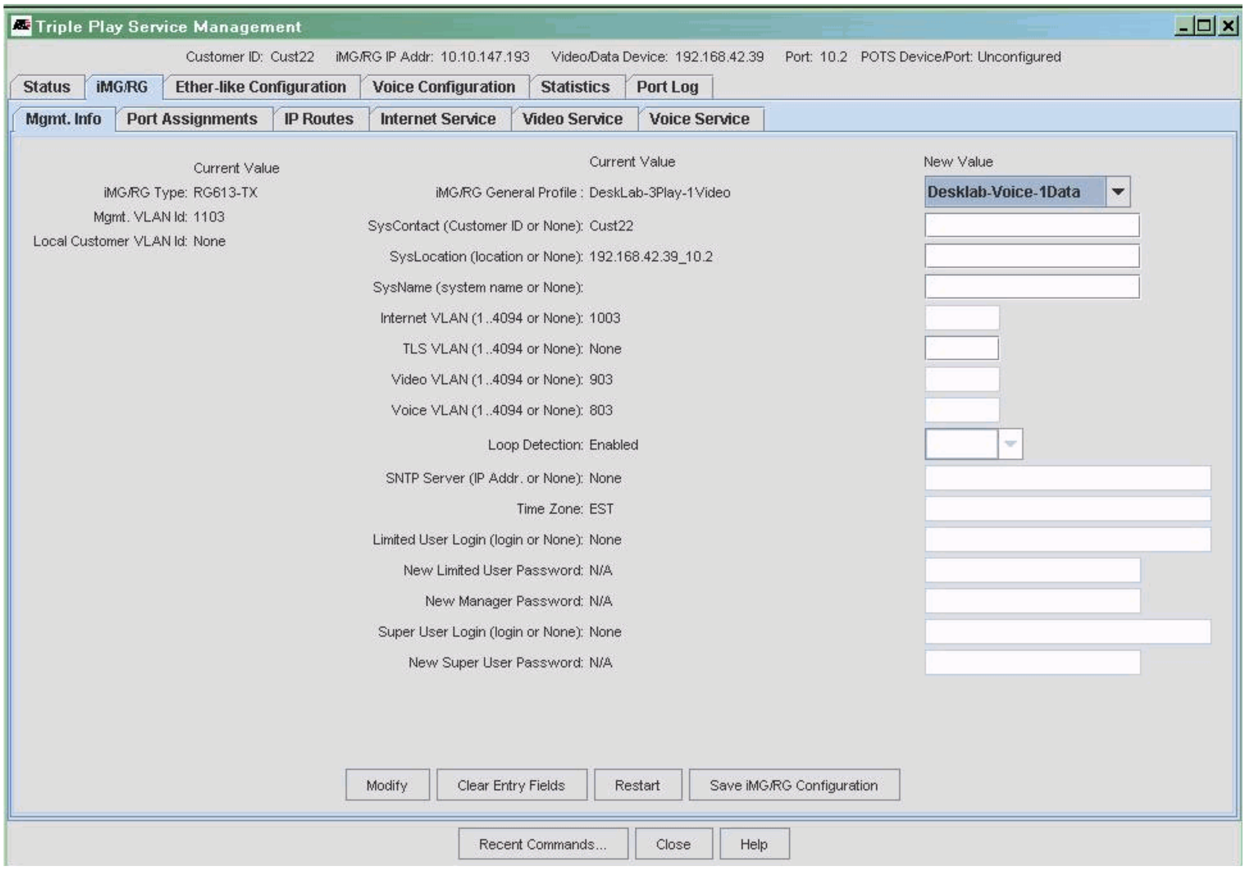
#	Current Value	New Value
1		
2		
3		
4		
5		
6		

FIGURE 21-67 Deleting Video Profile

5. Click **Modify**.

Note: At this point you could select Save iMG/RG Configuration, and the customer would have no video service but still have it configured on the RG.

6. Select the Mgmt. Info tab (still under the iMG/RG tab).
7. For the iMG/RG General Profile, select the double-play General Profile the customer will use. Refer to the following figure.



Customer ID: Cust22 iMG/RG IP Addr: 10.10.147.193 Video/Data Device: 192.168.42.39 Port: 10.2 POTS Device/Port: Unconfigured

Current Value
iMG/RG Type: RG613-TX
Mgmt. VLAN Id: 1103
Local Customer VLAN Id: None

	Current Value	New Value
iMG/RG General Profile :	DeskLab-3Play-1Video	Desklab-Voice-1Data
SysContact (Customer ID or None):	Cust22	
SysLocation (location or None):	192.168.42.39_10.2	
SysName (system name or None):		
Internet VLAN (1..4094 or None):	1003	
TLS VLAN (1..4094 or None):	None	
Video VLAN (1..4094 or None):	903	
Voice VLAN (1..4094 or None):	803	
Loop Detection:	Enabled	
SNTP Server (IP Addr. or None):	None	
Time Zone:	EST	
Limited User Login (login or None):	None	
New Limited User Password:	N/A	
New Manager Password:	N/A	
Super User Login (login or None):	None	
New Super User Password:	N/A	

FIGURE 21-68 Customer Using Profile for Double Play (no Video)

8. Select **Save iMG/RG Configuration**.
9. Back on the Status tab, click on **Update Customer Info**.
10. Note the results: any video connected to the RG will no longer work.
11. END OF PROCEDURE

21.15.6 Reprovision Existing iMG/RG so incorporated into AlliedView NMS

In this scenario, the iMG/RG has already been provisioned either locally or using the ZTC components. If the user wishes to take the existing iMG/RG and transfer control over to the NMS, the NMS will make a best effort and try to ensure that all of the features on the iMG/RG can be controlled by the NMS.

When transferring control over, the user should be aware of the following NMS features:

- The NMS shows only one service per LAN port.
- The NMS can’t tell the difference between bridged internet service and video without snooping, unless the service is named “InternetIP” or “VideoIP”.
- The NMS can’t tell the difference between bridged internet service and TLS, unless the service is named “InternetIP” or “TLSIP”.
- The NMS supports a single Internet service.
- The NMS only supports PPPoE on Internet service.
- The NMS only supports rate limiting on Internet service.
- All LAN ports are set as untagged.

- All service VLANs must be tagged on the WAN ports.
- Any parameters (especially voice) not supported by the NMS may or may not be preserved when changing over to the NMS.

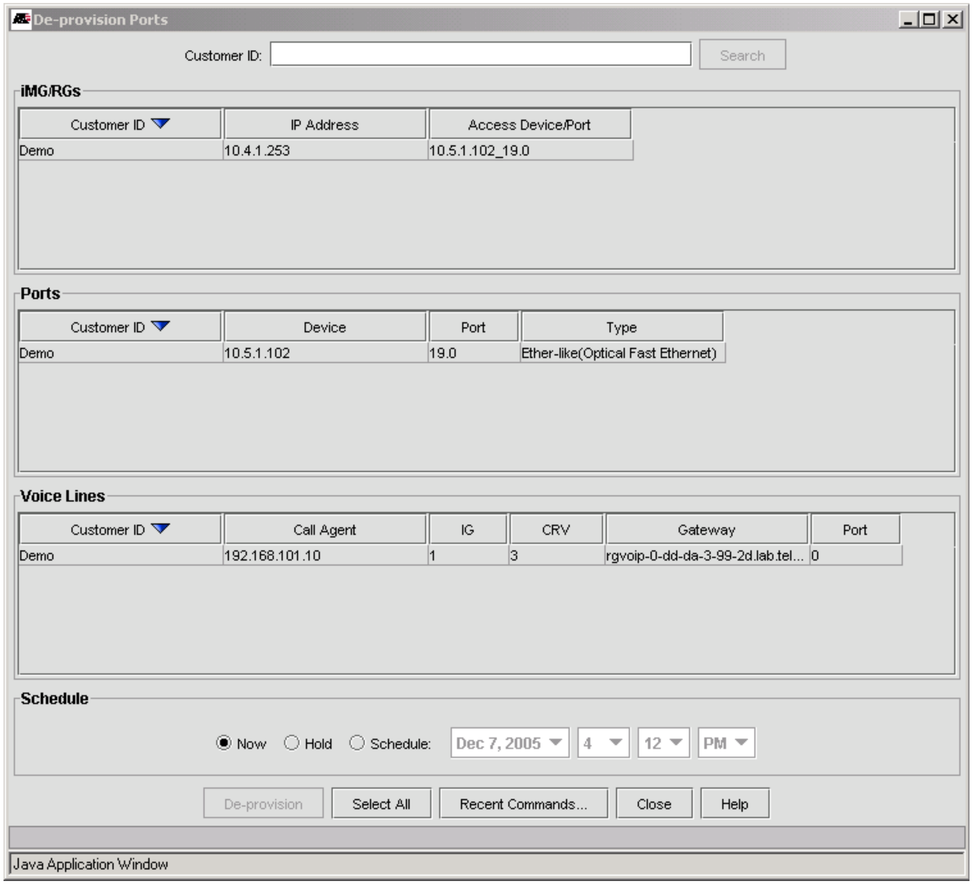
21.15.7 De-Provision iMG/RG from AlliedView NMS

21.15.7.1 Overview (Access Island and Open Access Considerations)

When the user wishes to de-provision the iMG/RG, there are two options:

- From the port table, select the port and then *Port -> De-provision Customer/port*
- From the iMG/RG table, select the iMG/RG and then *Operations -> De-provision Customer iMG/RG*

Either choice brings up the **De-provision Ports** form, as shown in Figure 21-69.



Customer ID:

iMG/RGs

Customer ID	IP Address	Access Device/Port
Demo	10.4.1.253	10.5.1.102_19.0

Ports

Customer ID	Device	Port	Type
Demo	10.5.1.102	19.0	Ether-like(Optical Fast Ethernet)

Voice Lines

Customer ID	Call Agent	IG	CRV	Gateway	Port
Demo	192.168.101.10	1	3	rgvoip-0-dd-da-3-99-2d.lab.tel...	0

Schedule

● Now ○ Hold ○ Schedule: Dec 7, 2005 4 12 PM

FIGURE 21-69 De provision Ports Form

There are three options for deletion:

- iMG/RG - Deletes the Customer ID and all associated profiles. The user can now provision a new Customer ID for the iMG /RG and build a service set from profiles.
- Ports (iMAP) - De-provisions the iMG/RG, the associated profiles, and the associated ports. If a POTS24 was being used to provide voice service, the POTS24 port would appear here as well.
- Voice Line - If there is a connection to the GenBand, the attributes associated with it are shown here. If more than one voice line is being used, all would appear here.

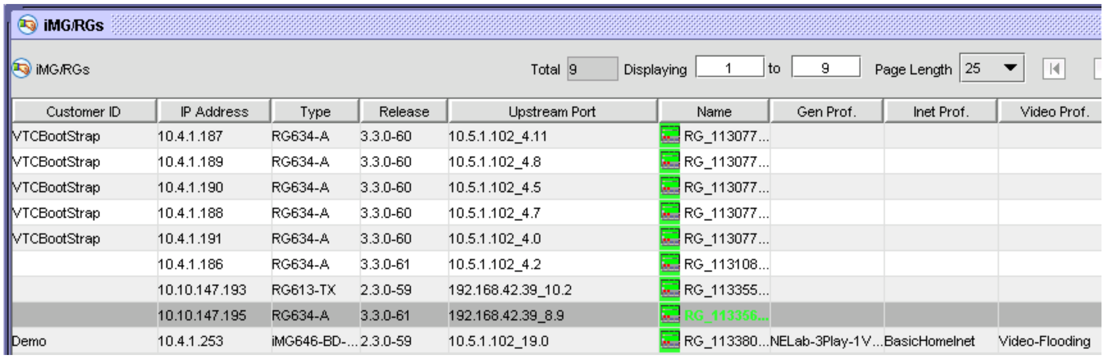
Moreover, choosing these options depends on what the user is trying to do:

- The user wishes to de-provision the RG (put back in the box), and then be able to re-provision the RG on the same Access Island. In this case, the RG, when taken out of the box and re-provisioned, would be using the same RGMgmt VLAN.
- The user wishes to de-provision the RG (put back in the box), and then be able to re-provision the RG on a different Access Island. In this case, the RG, when taken out of he box and re-provisioned, would need to start with the default (bootstrap) VLAN for DHCP discovery.
- The user has an open access model, and so he strategy depends on whether the same RGMgmt VLAN is used for all iMG/ RGs in the network.

21.15.7.2 De provision the iMG/RG (same Access Island)

To de-provision the iMG/RG, perform the following steps:

1. Find the RG you wish to de-provision (usually using the Customer ID from the iMG/RG table.).
2. Select the iMG/RG and then *Operations -> De-provision Customer iMG/RG*. The De-provision Port form appears.
3. Select the Customer ID option for all three panels, then click on **De-Provision**.
4. The RG will reboot.
5. In the iMG/RG table, the Customer ID is deleted and all profile information is deleted. Refer to Figure 21-70

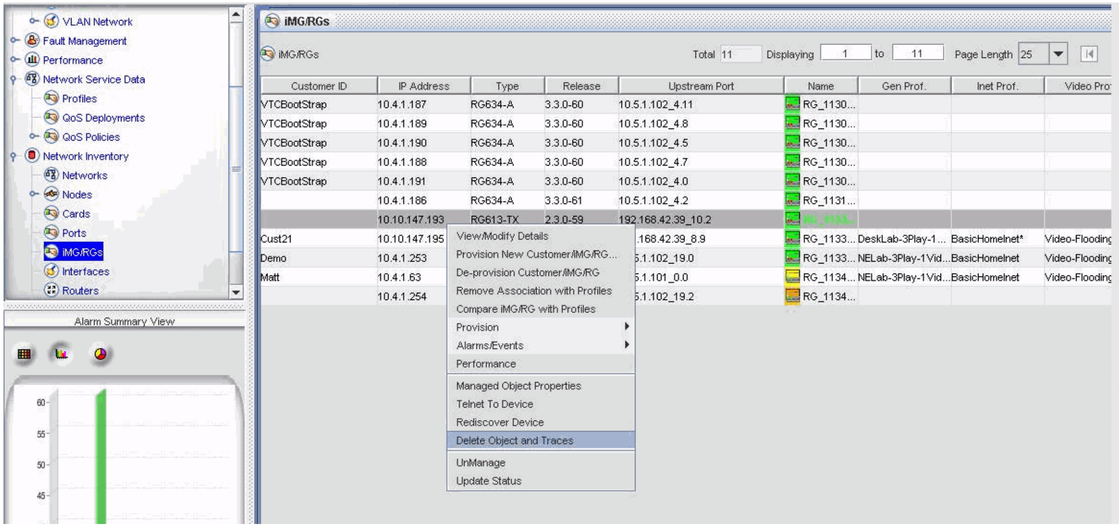


Customer ID	IP Address	Type	Release	Upstream Port	Name	Gen Prof.	Inet Prof.	Video Prof.
VTCBootStrap	10.4.1.187	RG634-A	3.3.0-60	10.5.1.102_4.11	RG_113077...			
VTCBootStrap	10.4.1.189	RG634-A	3.3.0-60	10.5.1.102_4.8	RG_113077...			
VTCBootStrap	10.4.1.190	RG634-A	3.3.0-60	10.5.1.102_4.5	RG_113077...			
VTCBootStrap	10.4.1.188	RG634-A	3.3.0-60	10.5.1.102_4.7	RG_113077...			
VTCBootStrap	10.4.1.191	RG634-A	3.3.0-60	10.5.1.102_4.0	RG_113077...			
	10.4.1.186	RG634-A	3.3.0-61	10.5.1.102_4.2	RG_113108...			
	10.10.147.193	RG613-TX	2.3.0-59	192.168.42.39_10.2	RG_113355...			
	10.10.147.195	RG634-A	3.3.0-61	192.168.42.39_8.9	RG_113356...			
Demo	10.4.1.253	iMG646-BD-...	2.3.0-59	10.5.1.102_19.0	RG_113380...	NELab-3Play-1V...	BasicHomeInet	Video-Flooding

FIGURE 21-70 iMG/RG Table after Deleting RG

6. To remove the port-RG association, right click on the RG and select **Delete Object and Traces**. Refer to the following figure.

Note: If iMG/RG equipment is to remain unprovisioned on this port temporarily (waiting for new customer to move in etc...), then the deletion of the RG object and traces is optional.



iMG/RGs Total 11 Displaying 1 to 11 Page Length 25

Customer ID	IP Address	Type	Release	Upstream Port	Name	Gen Prof.	Inet Prof.	Video Pro
VTCBootStrap	10.4.1.187	RG634-A	3.3.0-60	10.5.1.102_4.11	RG_1130...			
VTCBootStrap	10.4.1.189	RG634-A	3.3.0-60	10.5.1.102_4.8	RG_1130...			
VTCBootStrap	10.4.1.190	RG634-A	3.3.0-60	10.5.1.102_4.5	RG_1130...			
VTCBootStrap	10.4.1.188	RG634-A	3.3.0-60	10.5.1.102_4.7	RG_1130...			
VTCBootStrap	10.4.1.191	RG634-A	3.3.0-60	10.5.1.102_4.0	RG_1130...			
	10.4.1.186	RG634-A	3.3.0-61	10.5.1.102_4.2	RG_1131...			
	10.10.147.193	RG613-TX	2.3.0-59	192.168.42.39_10.2	RG_1133...			
Cust21	10.10.147.195			.168.42.39_8.9	RG_1133...	DeskLab-3Play-1...	BasicHomelnet*	Video-Flooding
Demo	10.4.1.253			5.1.102_19.0	RG_1133...	NELab-3Play-1Vid...	BasicHomelnet	Video-Flooding
Matt	10.4.1.63			5.1.101_0.0	RG_1134...	NELab-3Play-1Vid...	BasicHomelnet	Video-Flooding
	10.4.1.254			5.1.102_19.2	RG_1134...			

FIGURE 21-71 Delete RG-Port Association (Delete Object and Traces)

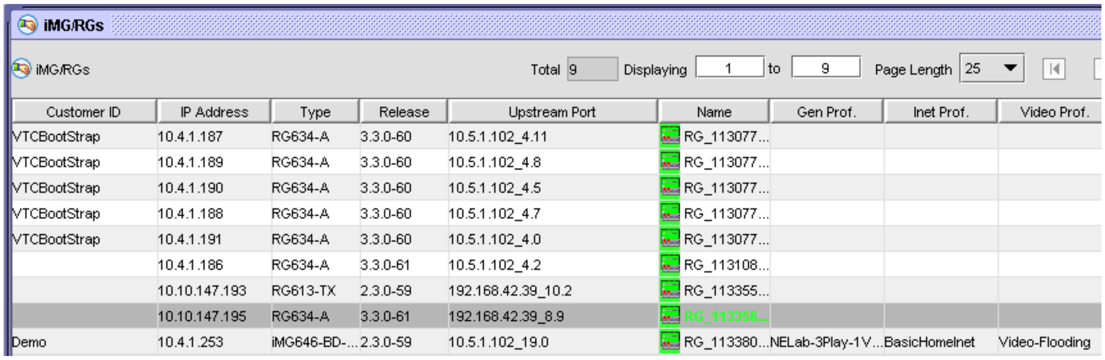
7. The user can now either:

- Place the iMG/RG back in its box for storage. When the RG is reconnected, it must be to a port in the **same** Access Island.
- Transfer the RG to another iMAP port in the same Access Island.

8. End of Procedure.

21.15.7.3 De-provision the iMG/RG (Different Access Island)

1. Find the RG you wish to de-provision (usually using the Customer ID from the iMG/RG table.).
2. Select the iMG/RG and then *Operations -> De-provision Customer iMG/RG*. The De-provision Port form appears.
3. Select the Customer ID option for the **iMG/RGs** and **Voice Lines** only, then click on **De-Provision**.
4. The RG will reboot.
5. In the iMG/RG table, the Customer ID is deleted and all profile information is deleted. Refer to Figure 21-72.

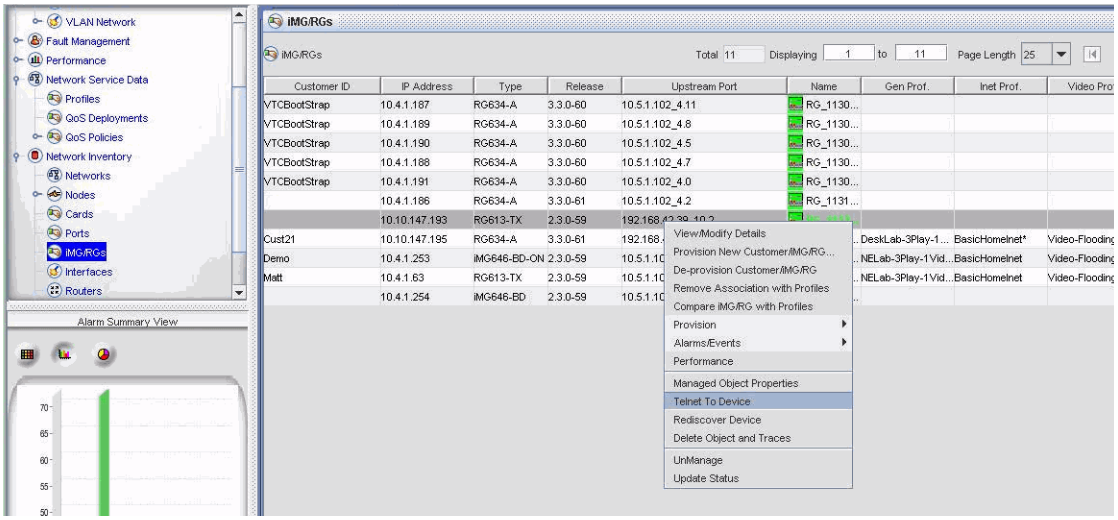

iMG/RGs

iMG/RGs Total 9 Displaying 1 to 9 Page Length 25

Customer ID	IP Address	Type	Release	Upstream Port	Name	Gen Prof.	Inet Prof.	Video Prof.
VTCBootStrap	10.4.1.187	RG634-A	3.3.0-60	10.5.1.102_4.11	RG_113077...			
VTCBootStrap	10.4.1.189	RG634-A	3.3.0-60	10.5.1.102_4.8	RG_113077...			
VTCBootStrap	10.4.1.190	RG634-A	3.3.0-60	10.5.1.102_4.5	RG_113077...			
VTCBootStrap	10.4.1.188	RG634-A	3.3.0-60	10.5.1.102_4.7	RG_113077...			
VTCBootStrap	10.4.1.191	RG634-A	3.3.0-60	10.5.1.102_4.0	RG_113077...			
	10.4.1.186	RG634-A	3.3.0-61	10.5.1.102_4.2	RG_113108...			
	10.10.147.193	RG613-TX	2.3.0-59	192.168.42.39_10.2	RG_113355...			
	10.10.147.195	RG634-A	3.3.0-61	192.168.42.39_8.9	RG_113356...			
Demo	10.4.1.253	iMG646-BD-...	2.3.0-59	10.5.1.102_19.0	RG_113380...	NELab-3Play-1V...	BasicHomelnet	Video-Flooding

FIGURE 21-72 iMG/RG Table after Deleting RG

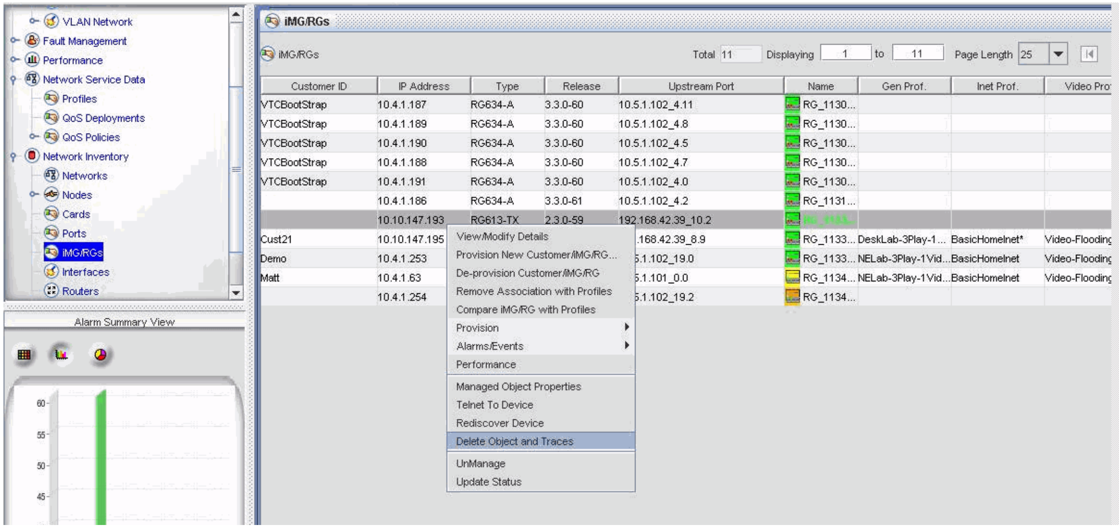
6. Access the device using telnet. Right click on the iMG/RG in the iMG/RG table and select **Telnet to Device**. Refer to the following figure.



Customer ID	IP Address	Type	Release	Upstream Port	Name	Gen Prof.	Inet Prof.	Video Pro
VTCBootStrap	10.4.1.187	RG634-A	3.3.0-60	10.5.1.102_4.11	RG_1130...			
VTCBootStrap	10.4.1.189	RG634-A	3.3.0-60	10.5.1.102_4.8	RG_1130...			
VTCBootStrap	10.4.1.190	RG634-A	3.3.0-60	10.5.1.102_4.5	RG_1130...			
VTCBootStrap	10.4.1.188	RG634-A	3.3.0-60	10.5.1.102_4.7	RG_1130...			
VTCBootStrap	10.4.1.191	RG634-A	3.3.0-60	10.5.1.102_4.0	RG_1130...			
	10.4.1.186	RG634-A	3.3.0-61	10.5.1.102_4.2	RG_1131...			
	10.10.147.193	RG613-TX	2.3.0-59	192.168.42.39_10.2				
Cust21	10.10.147.195	RG634-A	3.3.0-61	192.168.		DeskLab-3Play-1...	BasicHomeInet*	Video-Flooding
Demo	10.4.1.253	iMG646-BD-ON	2.3.0-59	10.5.1.1		NELab-3Play-1Vid...	BasicHomeInet	Video-Flooding
Matt	10.4.1.63	RG613-TX	2.3.0-59	10.5.1.1		NELab-3Play-1Vid...	BasicHomeInet	Video-Flooding
	10.4.1.254	iMG646-BD	2.3.0-59	10.5.1.1				

FIGURE 21-73 Using telnet to Access the RG

7. Login to the iMG/RG.
8. Set back to factory defaults (>sys config set factory)
9. You can now unplug the RG and place it back in its box.
10. Return to the De-Provision Ports Form.
11. This time select the Ports panel.
12. Right click on the iMG/RG and select **Delete Object and Traces**, as shown in the following figure.



Customer ID	IP Address	Type	Release	Upstream Port	Name	Gen Prof.	Inet Prof.	Video Pro
VTCBootStrap	10.4.1.187	RG634-A	3.3.0-60	10.5.1.102_4.11	RG_1130...			
VTCBootStrap	10.4.1.189	RG634-A	3.3.0-60	10.5.1.102_4.8	RG_1130...			
VTCBootStrap	10.4.1.190	RG634-A	3.3.0-60	10.5.1.102_4.5	RG_1130...			
VTCBootStrap	10.4.1.188	RG634-A	3.3.0-60	10.5.1.102_4.7	RG_1130...			
VTCBootStrap	10.4.1.191	RG634-A	3.3.0-60	10.5.1.102_4.0	RG_1130...			
	10.4.1.186	RG634-A	3.3.0-61	10.5.1.102_4.2	RG_1131...			
	10.10.147.193	RG613-TX	2.3.0-59	192.168.42.39_10.2				
Cust21	10.10.147.195			.168.42.39_8.9	RG_1133...	DeskLab-3Play-1...	BasicHomeInet*	Video-Flooding
Demo	10.4.1.253			5.1.102_19.0	RG_1133...	NELab-3Play-1Vid...	BasicHomeInet	Video-Flooding
Matt	10.4.1.63			5.1.101_0.0	RG_1134...	NELab-3Play-1Vid...	BasicHomeInet	Video-Flooding
	10.4.1.254			5.1.102_19.2	RG_1134...			

FIGURE 21-74 Delete RG-Port Association (Delete Object and Traces)

13. When the RG is reconnected, the default VLAN for the RG is used at the start for DHCP discovery. Therefore, this would most likely be for connecting the RG to an iMAP that is in **any** Access Island than where it was de-provisioned.
14. END OF PROCEDURE

21.15.7.4 De provision the iMG/RG (Open Access)

In the Open Access Model, it is the use of the RGMgmt VLAN that determines the strategy to follow:

- If the iMG/RG is to be reconfigured where the same RGMgmt VLAN is used, the iMG/RG would not be set back to its factory settings before re-provisioning, similar to De provision the iMG/RG (same Access Island).
- If the iMG/RG is to be reconfigured where a different RGMgmt VLAN is used, the iMG/RG would be set back to its factory settings before re-provisioning, similar to De-provision the iMG/RG (Different Access Island).

21.15.8 Changing a Customer ID

21.15.8.1 Overview

Section Naming Convention for Customer IDs (Triple Play Form) listed the naming conventions to follow for Customer IDs. To change a Customer ID, the administrator must enter the changed ID for all three configuration areas (tabs) on the Triple Play Service Management form.

- Connection Type - Ether-like, ADSL, or ONU
- iMG/RG
- Voice

All three are filled in the Service Management form.

Caution: *The customer ID value must be filled in for all three areas before the form is closed, and the value must be the same for all three areas. Otherwise, the value will not be propagated to all three areas correctly.*

21.15.8.2 Procedure

1. Bring up the Triple Service Management Form for the Customer ID. To do this, select and right click on **View/Modify Details** with one of the following:

- The row with the current Customer ID from the Ports Inventory table.
- The row with the current Customer ID from the iMG/RG Inventory table
- The iMG/RG icon from the relevant IP Network MAP

2. Select the connection type tab, such as **Ether-like Configuration -> General**, and fill in the changed Customer ID.
3. Select the **iMG/RG -> Mgmt. Info** tab, and fill in the changed Customer ID.
4. Select the **Voice Configuration - > protocol Info** tab, and fill in the changed Customer ID.

Note: *The customer ID is not on the CPE sub-tab for the Voice Configuration.*

5. Click on the **Modify** button to make the changes take effect.
6. You can now close the Form.

21.15.9 iMG/RG Recovery

This procedure is used when the iMG/RG has gone into Recovery Mode. This could happen, for example, if during the middle of an upgrade procedure the iMG/RG lost power and as a result went into Recovery mode.

Note: *The iMG/RG will have a constant red light on when it has entered Recovery mode.*

There are two procedures that can be used, depending on whether the existing RG is to be recovered or a new iMG.RG is to be swapped.

21.15.9.1 Recover Existing iMG/RG

1. Add the Bootstrap VLAN to the subscriber’s iMAP port.
2. The iMG/RG should be able to contact a DHCP server and get an IP address
3. Using a tool called the Windows Loader, input the iMG/RG IP Address and the telnet password, default value “friend”.

Note: For information on the Windows Loader, refer to the Software Reference Manual for the AT-RG600. This document can be found on the Allied Telesis website.

4. The RG should then reboot and go back to Normal mode, with the bootstrap loading on the RG-mgmt VLAN.
5. Using the AlliedView NMS application (Device Backup/Restore), restore the last saved configuration file for the RG.
6. The bootstrap VLAN can now be removed from the subscriber's port.

21.15.10 Recover using new Hardware

Use this procedure to replace suspected bad iMG hardware unit.

21.15.10.1 Prerequisites

- Ensure iMG hardware model of new unit matches model of unit to be replaced (old unit).
- Ensure the new iMG unit has not been previously managed by the target NMS, to prevent possible complications.
- Ensure iMG software boot load release matches release of iMG to be replaced.
- Ensure the new iMG unit contains only the "factory" system configuration file.
- Ensure the old iMG configuration has been backed up recently. If a current backup is not available, do **not** use the procedure in Procedure. Instead, do the following:
    1. Record all subscriber configuration information
    2. Deprovision the subscriber (refer to De-Provision iMG/RG from AlliedView NMS).
    3. Provision using a new iMG hardware unit, and the recorded information (refer to Triple Play Examples).

21.15.10.2 Procedure

1. Add the Bootstrap VLAN to the subscriber's iMAP port.
2. Swap the existing iMG/RG with a new one.
    1. Power off the old iMG unit, and replace with new unit, connecting all cables.
    2. Power on the new unit.
3. The iMG/RG should be able to contact a DHCP server and get an IP address and go through the bootstrap process.
4. The AlliedView NMS should discover the new iMG/RG and restore the last saved config file automatically.
5. The AlliedView NMS should then remove the bootstrap VLAN automatically.
6. Verify iMG management and all provisioned services.

21.15.11 Configuring multi-service VLAN

For a description of a multi-service VLAN model, refer to Configuration 6 - Multi-Service VLAN. This subsection gives procedures that involve creating three possible configurations. For all of the procedures the following apply:

- The port configuration for each IMG is the same (two voice, two video, one data). This allows the same General profile to be used for all configurations, even if the type of iMG (EPON, FX, ADSL) is different.
- The VLANs involved should have already been created.
- The port Profile should have already been created, although it is not included here.

21.15.11.1 Creating a Voice and Video/Data VLAN (Configuration 1)

In this configuration, the Voice VLAN is on a separate VLAN, but video and data share a single VLAN. Refer to the following figure and notes in Configuring multi-service VLAN before performing the procedure.

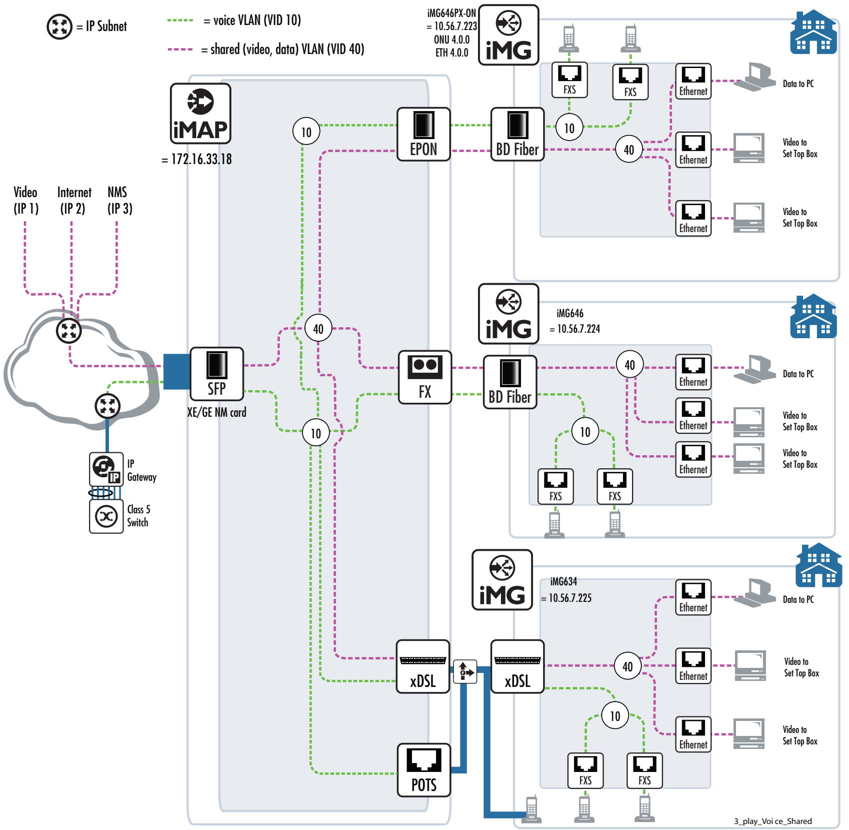
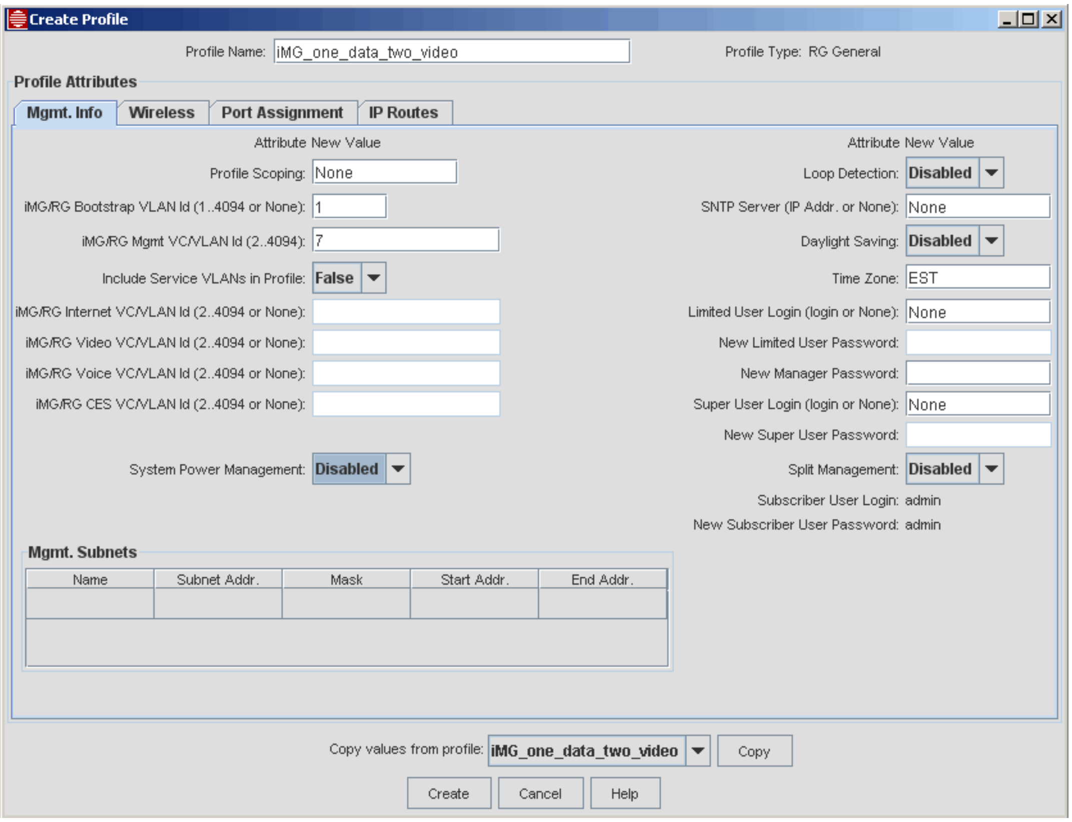


FIGURE 21-75 Multi-service (Video, Data) VLAN - Configuration 1

1. Create the appropriate iMG profiles. Refer to the following table and figures.

TABLE 21-8 iMG Forms for Voice, Video/Data VLAN Configuration

Form	Name	Attributes	Reference
General	iMG_one_data_two_video		Figure 21-76 - Mgmt. Info Figure 21-77 - Port Assignment
Internet	iMG_data_shared_VLAN_vidoe		Figure 21-78
Video	iMG_video_shared_data		Figure 21-79
Voice	iMG_MGCP_two_line	Since this is not a shared VLAN and uses MGCP, an existing form can be used	Figure 21-80



Profile Name: iMG_one_data_two_video

Profile Type: RG General

Attribute	New Value
Profile Scoping:	None
iMG/RG Bootstrap VLAN Id (1..4094 or None):	1
iMG/RG Mgmt VC/VLAN Id (2..4094):	7
Include Service VLANs in Profile:	False
iMG/RG Internet VC/VLAN Id (2..4094 or None):	
iMG/RG Video VC/VLAN Id (2..4094 or None):	
iMG/RG Voice VC/VLAN Id (2..4094 or None):	
iMG/RG CES VC/VLAN Id (2..4094 or None):	
System Power Management:	Disabled

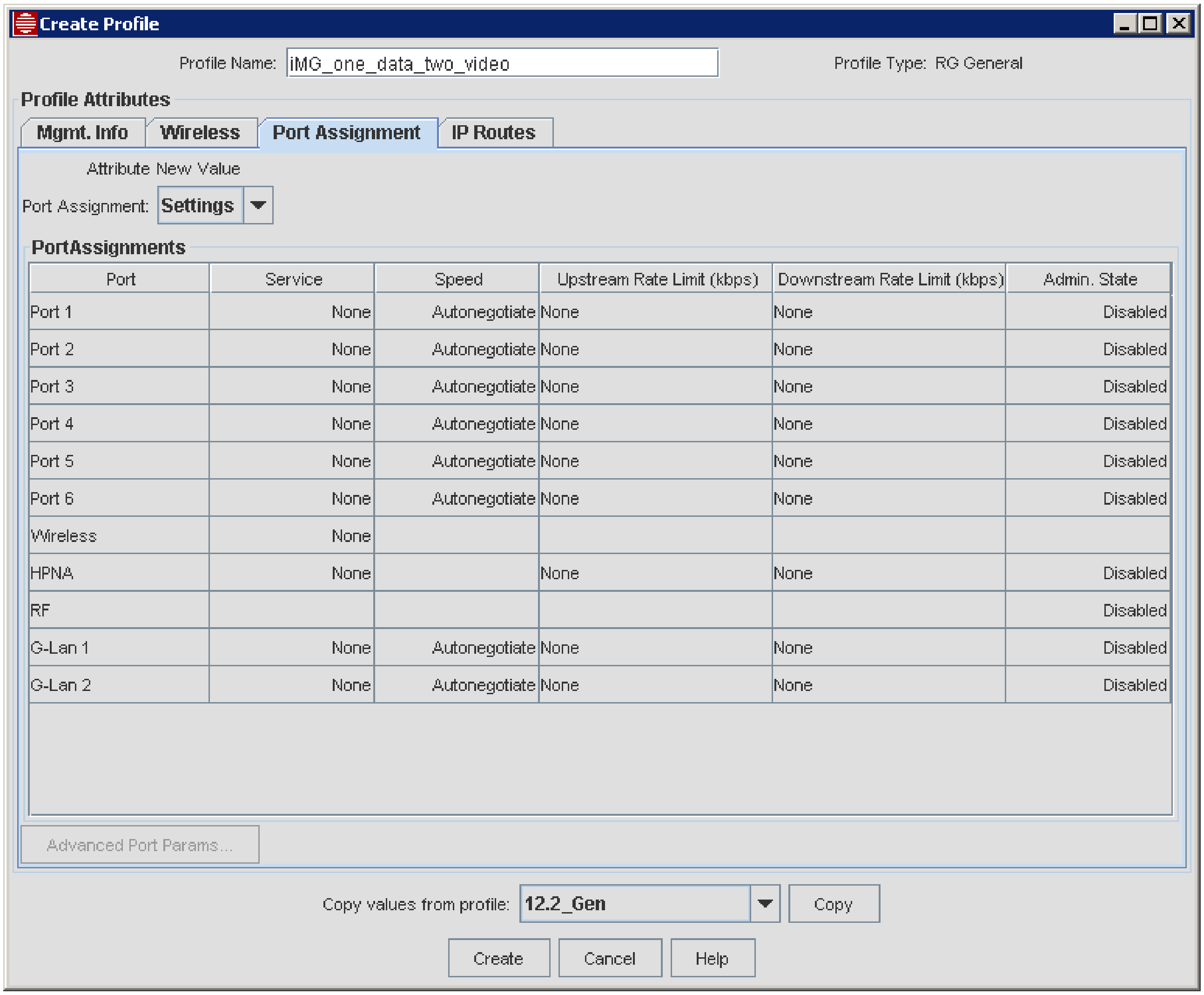
Attribute	New Value
Loop Detection:	Disabled
SNTP Server (IP Addr. or None):	None
Daylight Saving:	Disabled
Time Zone:	EST
Limited User Login (login or None):	None
New Limited User Password:	
New Manager Password:	
Super User Login (login or None):	None
New Super User Password:	
Split Management:	Disabled
Subscriber User Login:	admin
New Subscriber User Password:	admin

Mgmt. Subnets

Name	Subnet Addr.	Mask	Start Addr.	End Addr.

Copy values from profile: iMG_one_data_two_video

FIGURE 21-76 General Form for Multi-service VLAN - Mgmt. Info Tab



Profile Name: iMG_one_data_two_video

Profile Type: RG General

Profile Attributes

Attribute New Value

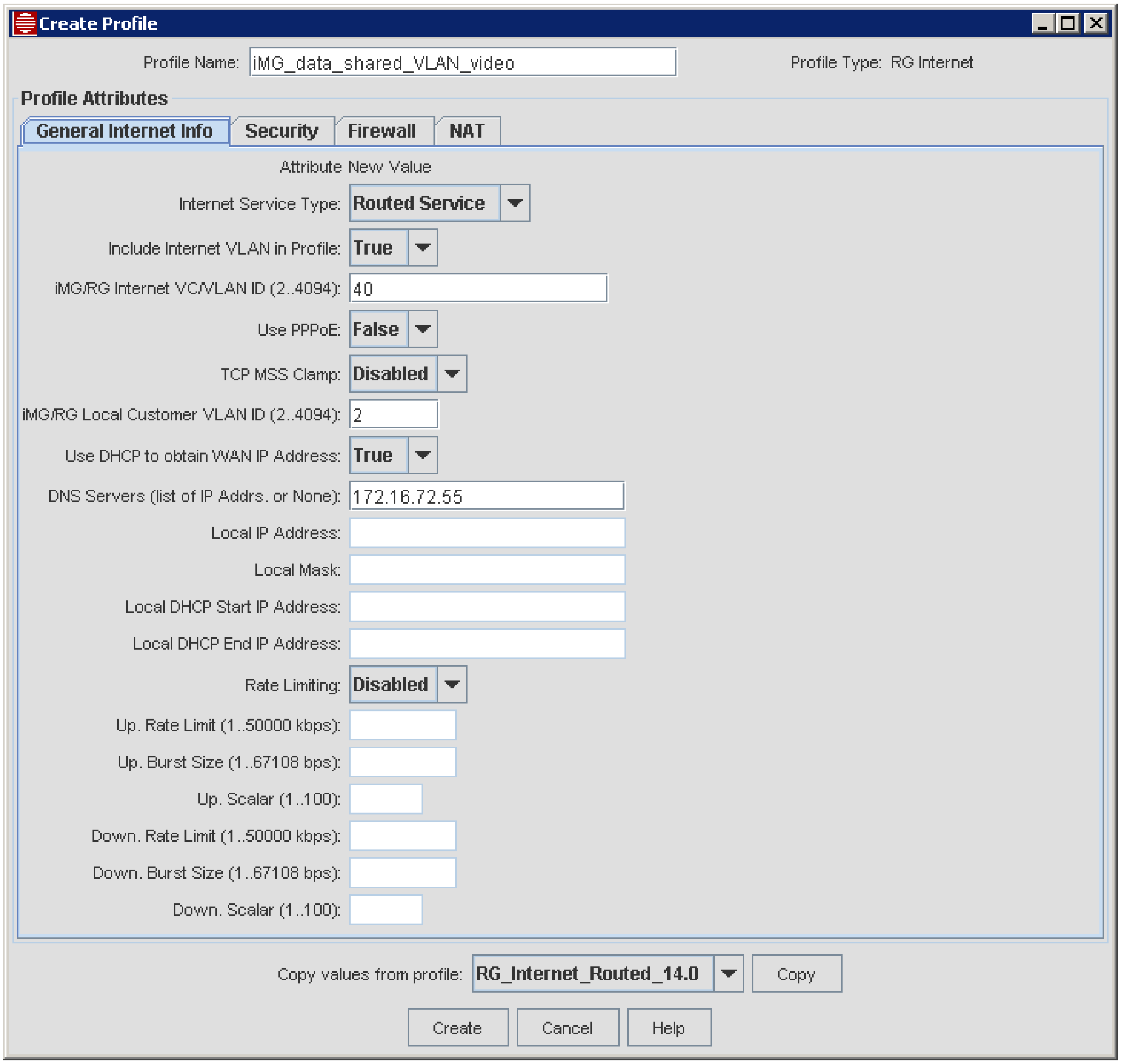
Port Assignment: Settings

PortAssignments

Port	Service	Speed	Upstream Rate Limit (kbps)	Downstream Rate Limit (kbps)	Admin. State
Port 1	None	Autonegotiate	None	None	Disabled
Port 2	None	Autonegotiate	None	None	Disabled
Port 3	None	Autonegotiate	None	None	Disabled
Port 4	None	Autonegotiate	None	None	Disabled
Port 5	None	Autonegotiate	None	None	Disabled
Port 6	None	Autonegotiate	None	None	Disabled
Wireless	None				
HPNA	None		None	None	Disabled
RF					Disabled
G-Lan 1	None	Autonegotiate	None	None	Disabled
G-Lan 2	None	Autonegotiate	None	None	Disabled

Copy values from profile: 12.2_Gen

FIGURE 21-77 General Form for Multi-service VLAN - Port Assignment Tab



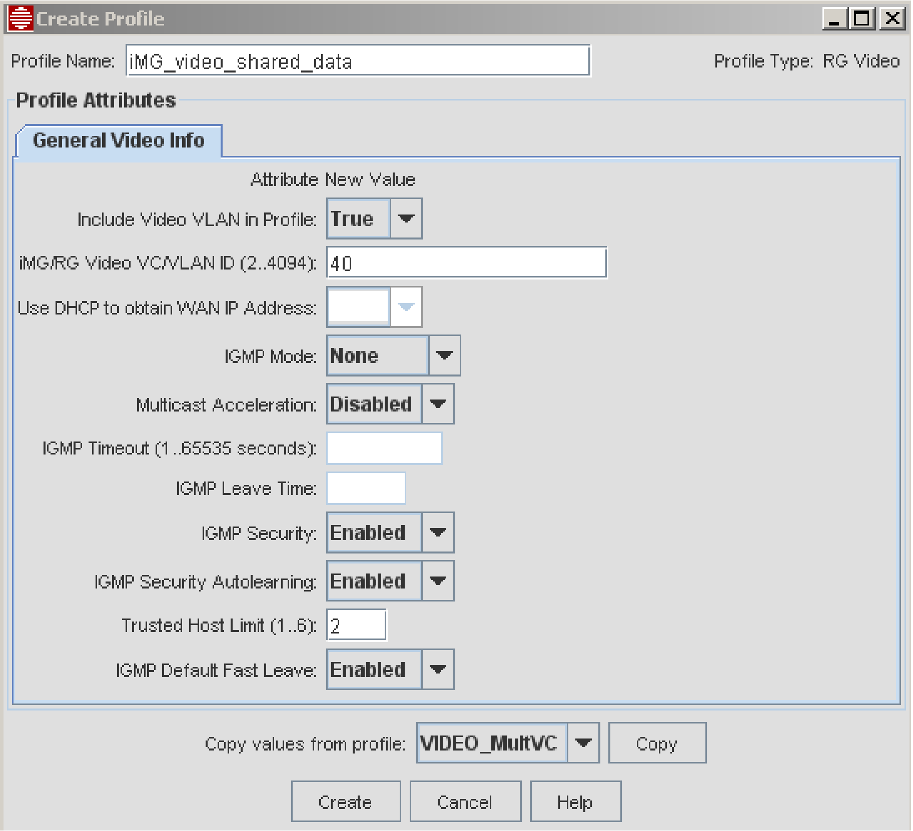
Profile Name: iMG_data_shared_VLAN_video

Profile Type: RG Internet

Attribute	New Value
Internet Service Type:	Routed Service
Include Internet VLAN in Profile:	True
iMG/RG Internet VC/VLAN ID (2..4094):	40
Use PPPoE:	False
TCP MSS Clamp:	Disabled
iMG/RG Local Customer VLAN ID (2..4094):	2
Use DHCP to obtain WAN IP Address:	True
DNS Servers (list of IP Addrs. or None):	172.16.72.55
Local IP Address:	
Local Mask:	
Local DHCP Start IP Address:	
Local DHCP End IP Address:	
Rate Limiting:	Disabled
Up. Rate Limit (1..50000 kbps):	
Up. Burst Size (1..67108 bps):	
Up. Scalar (1..100):	
Down. Rate Limit (1..50000 kbps):	
Down. Burst Size (1..67108 bps):	
Down. Scalar (1..100):	

Copy values from profile: RG_Internet_Routed_14.0

FIGURE 21-78 Internet Form for Multi-service VLAN - General Internet Info Tab - Configuration 1



Create Profile

Profile Name: iMG_video_shared_data

Profile Type: RG Video

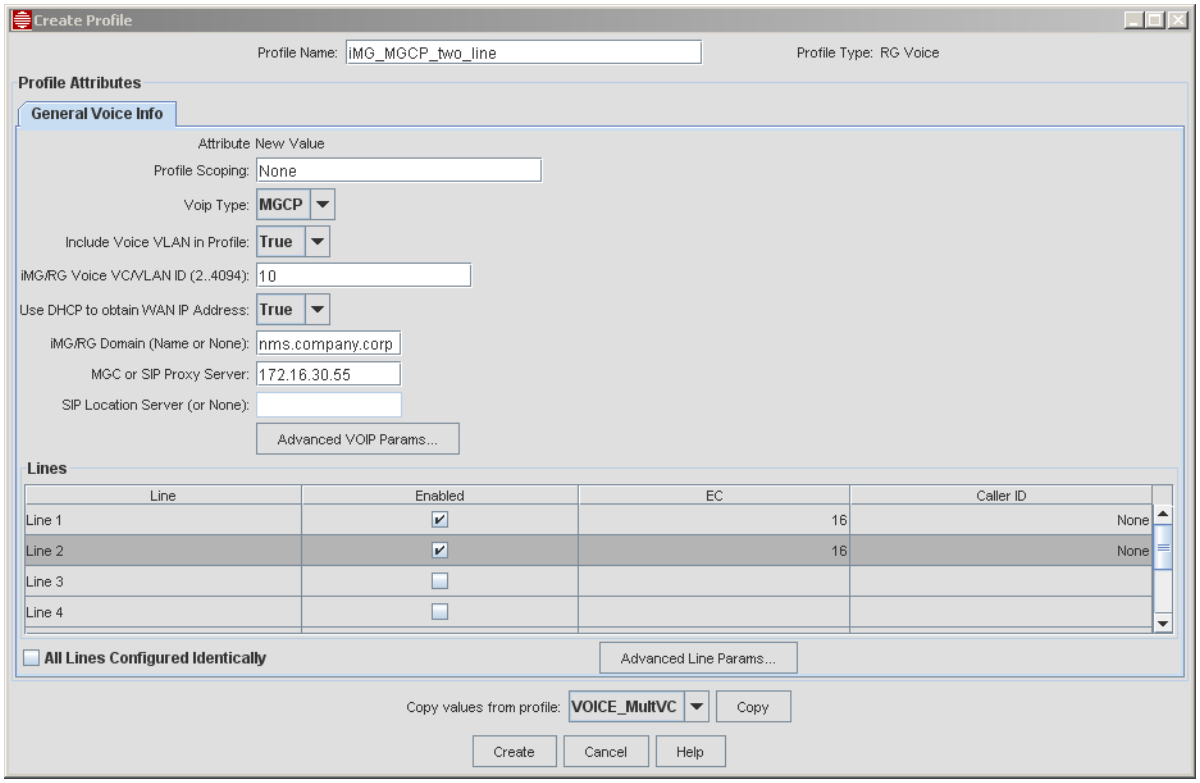
Profile Attributes

General Video Info

Attribute	New Value
Include Video VLAN in Profile:	True
iMG/RG Video VC/VLAN ID (2..4094):	40
Use DHCP to obtain WAN IP Address:	
IGMP Mode:	None
Multicast Acceleration:	Disabled
IGMP Timeout (1..65535 seconds):	
IGMP Leave Time:	
IGMP Security:	Enabled
IGMP Security Autolearning:	Enabled
Trusted Host Limit (1..6):	2
IGMP Default Fast Leave:	Enabled

Copy values from profile: VIDEO_MultVC

FIGURE 21-79 Video Form for Multi-service VLAN - Configuration 1



Profile Name: iMG_MGCP_two_line

Profile Type: RG Voice

Profile Scoping: None

Voip Type: MGCP

Include Voice VLAN in Profile: True

iMG/RG Voice VC/VLAN ID (2..4094): 10

Use DHCP to obtain WAN IP Address: True

iMG/RG Domain (Name or None): nms.company.corp

MGC or SIP Proxy Server: 172.16.30.55

SIP Location Server (or None):

Line	Enabled	EC	Caller ID
Line 1	☑	16	None
Line 2	☑	16	None
Line 3	□		
Line 4	□		

□ All Lines Configured Identically

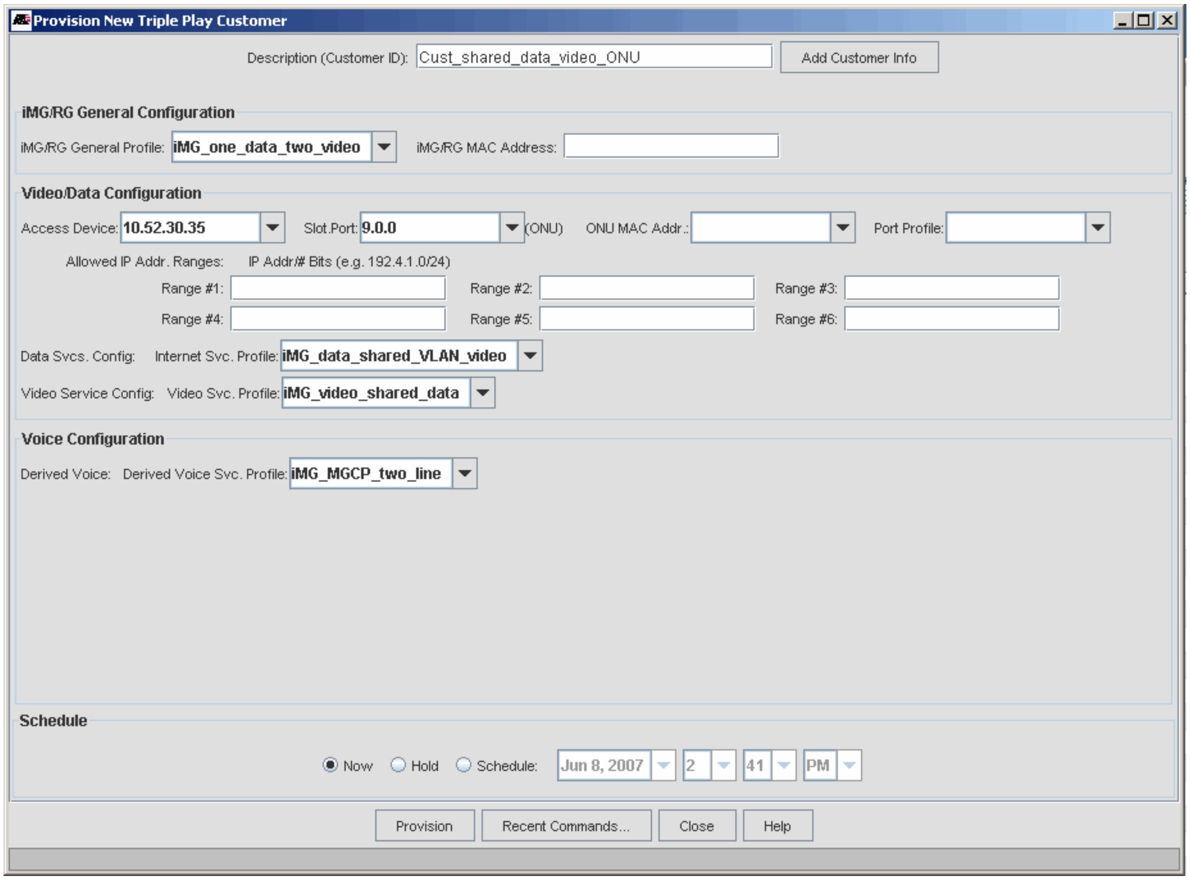
Copy values from profile: VOICE_MultVC

FIGURE 21-80 Voice Form for Multi-service VLAN - Configuration 1

2. Data fill the Triple-Play Form. Since there are three different customers and types of interfaces, the Customer ID for each must be unique, and the slot.Port will be different. (The iMAP could be the same if all of the interface cards were on the same iMAP. Refer to the following table.)

TABLE 21-9 Triple Play Forms for Voice, Video/Data VLAN Configuration

iMG Type	Attributes	Reference
EPON (iMG646PX-ON)		Figure 21-81 - Mgmt. Info
FX (iMG646)		Figure 21-82
ADSL (iMG634)		Figure 21-83



Provision New Triple Play Customer

Description (Customer ID): Cust_shared_data_video_ONU

iMG/RG General Configuration

iMG/RG General Profile: iMG_one_data_two_video

iMG/RG MAC Address:

Video/Data Configuration

Access Device: 10.52.30.35

Slot.Port: 9.0.0 (ONU)

ONU MAC Addr.:

Port Profile:

Allowed IP Addr. Ranges: IP Addr/# Bits (e.g. 192.4.1.0/24)

Range #1: Range #2: Range #3:

Range #4: Range #5: Range #6:

Data Svcs. Config: Internet Svc. Profile: iMG_data_shared_VLAN_video

Video Service Config: Video Svc. Profile: iMG_video_shared_data

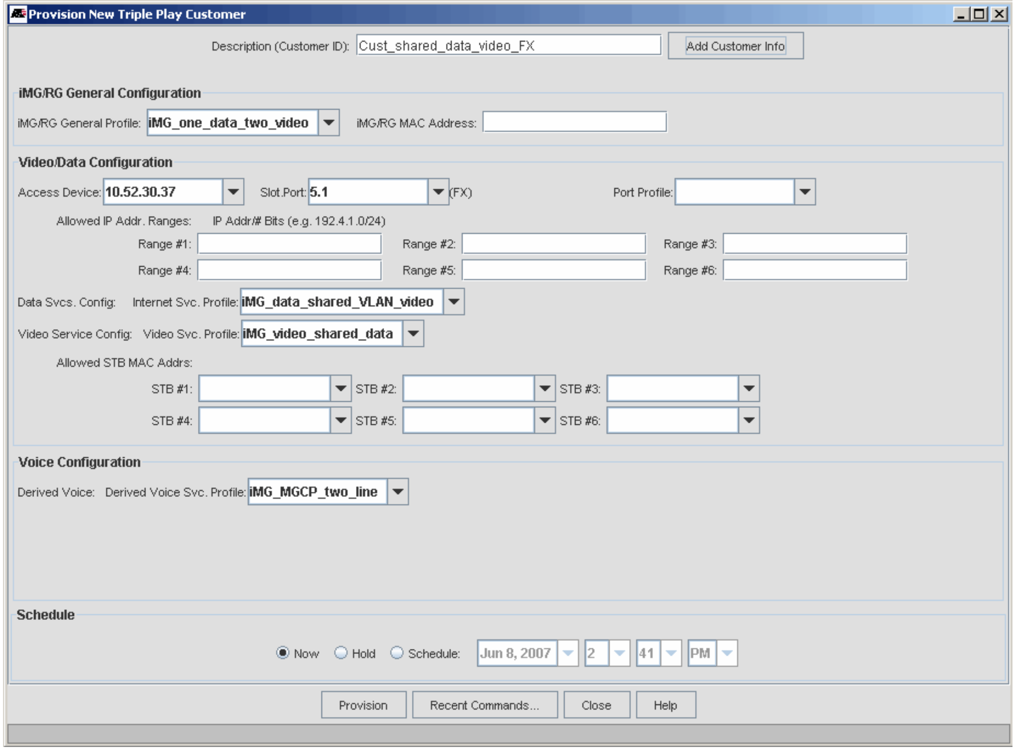
Voice Configuration

Derived Voice: Derived Voice Svc. Profile: iMG_MGCP_two_line

Schedule

● Now ○ Hold ○ Schedule: Jun 8, 2007 2 41 PM

FIGURE 21-81 Triple-Play Form EPON Interface - Configuration 1



Provision New Triple Play Customer

Description (Customer ID): Cust_shared_data_video_FX

iMG/RG General Configuration

iMG/RG General Profile: iMG_one_data_two_video

iMG/RG MAC Address:

Video/Data Configuration

Access Device: 10.52.30.37

Slot.Port: 5.1 (FX)

Port Profile:

Allowed IP Addr. Ranges: IP Addr/# Bits (e.g. 192.4.1.0/24)

Range #1: Range #2: Range #3:

Range #4: Range #5: Range #6:

Data Svcs. Config: Internet Svc. Profile: iMG_data_shared_VLAN_video

Video Service Config: Video Svc. Profile: iMG_video_shared_data

Allowed STB MAC Addrs:

STB #1: STB #2: STB #3:

STB #4: STB #5: STB #6:

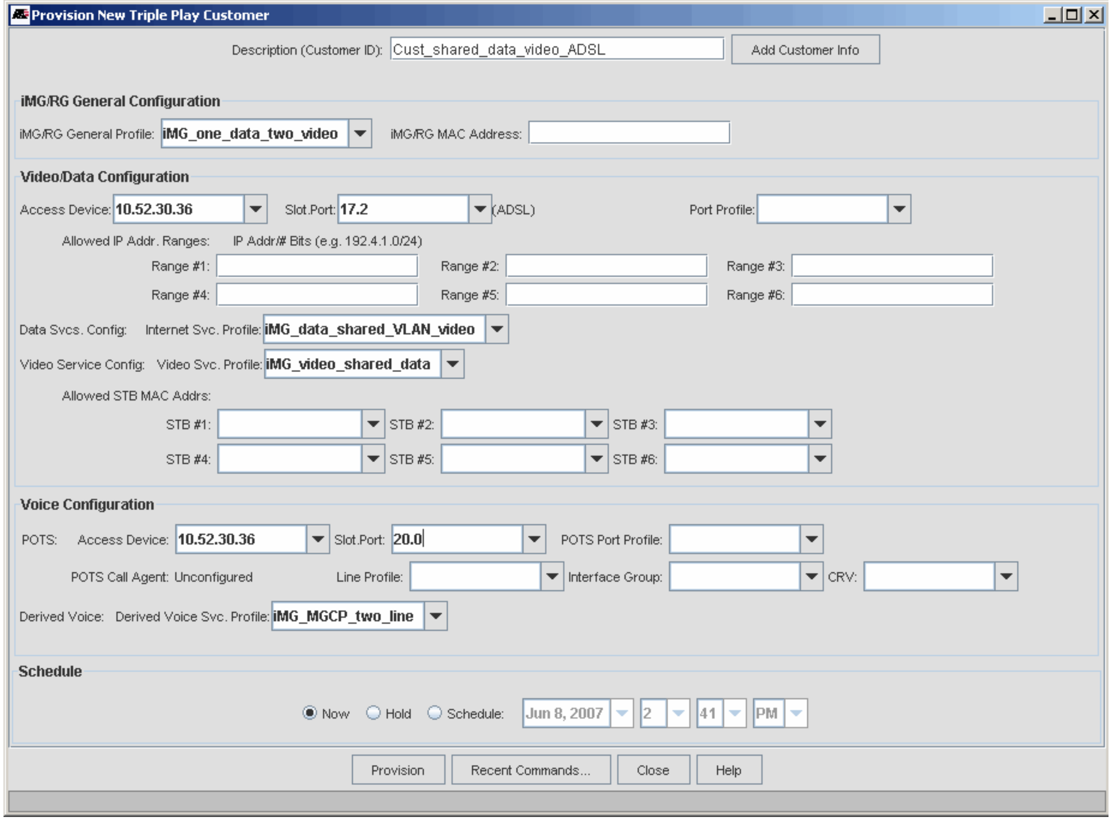
Voice Configuration

Derived Voice: Derived Voice Svc. Profile: iMG_MGCP_two_line

Schedule

● Now ○ Hold ○ Schedule: Jun 8, 2007 2 41 PM

FIGURE 21-82 Triple-Play Form FX Interface - Configuration 1



Provision New Triple Play Customer

Description (Customer ID): Cust_shared_data_video_ADSL

iMG/RG General Configuration

iMG/RG General Profile: iMG_one_data_two_video

iMG/RG MAC Address:

Video/Data Configuration

Access Device: 10.52.30.36

Slot.Port: 17.2 (ADSL)

Port Profile:

Allowed IP Addr. Ranges: IP Addr/# Bits (e.g. 192.4.1.0/24)

Range #1: Range #2: Range #3:

Range #4: Range #5: Range #6:

Data Svcs. Config: Internet Svc. Profile: iMG_data_shared_VLAN_video

Video Service Config: Video Svc. Profile: iMG_video_shared_data

Allowed STB MAC Addrs:

STB #1: STB #2: STB #3:

STB #4: STB #5: STB #6:

Voice Configuration

POTS: Access Device: 10.52.30.36

Slot.Port: 20.0

POTS Port Profile:

POTS Call Agent: Unconfigured

Line Profile: Interface Group: CRV:

Derived Voice: Derived Voice Svc. Profile: iMG_MGCP_two_line

Schedule

● Now ○ Hold ○ Schedule: Jun 8, 2007 2 41 PM

FIGURE 21-83 Triple-Play Form ADSL Interface - Configuration 1

21.15.11.2 Creating a Data and Video/Voice VLAN (Configuration 2)

In this configuration, the Data VLAN is on a separate VLAN, and video and voice share a single VLAN. Refer to the following figure and notes in Configuring multi-service VLAN before performing the procedure.

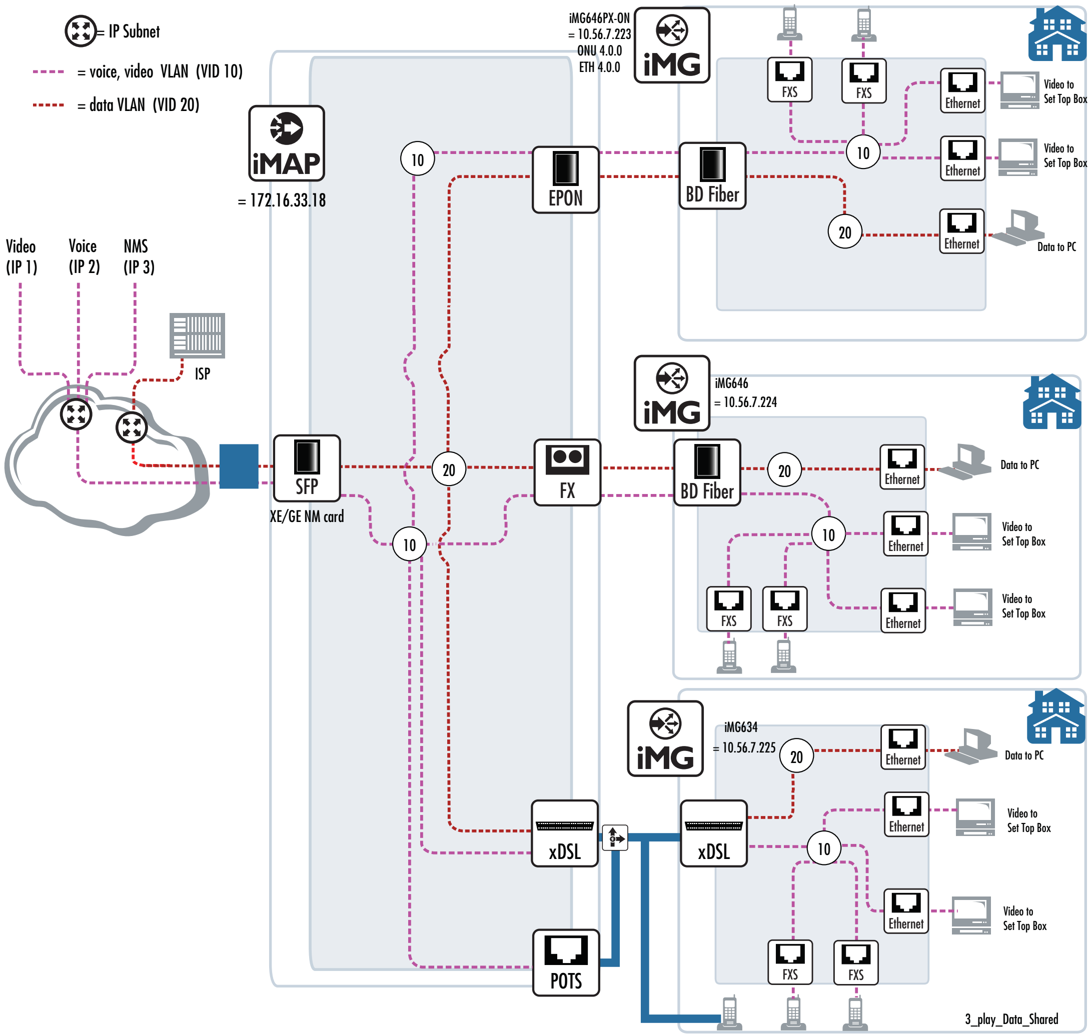
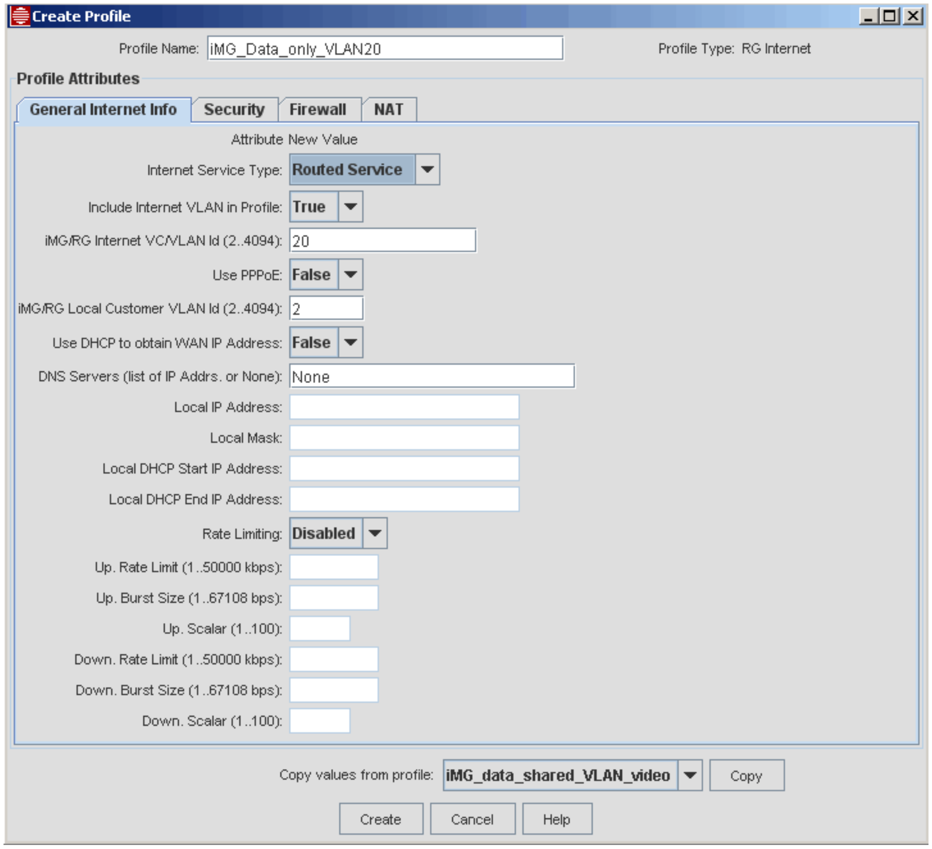


FIGURE 21-84 Multi-service (Video, Video) VLAN (Configuration 2)

1. Create the appropriate iMG profiles. Refer to the following table and figures.

TABLE 21-10 iMG Forms for Voice, Video/Data VLAN (Configuration) 2

Form	Name	Attributes	Reference
General	iMG_one_data_two_video	Since the port and VLAN configuration is the same for all iMGs, the same General Form is used in all configurations	Figure 21-76 - Mgmt. Info Figure 21-77 - Port Assignment
Internet	iMG_Data_only_VLAN20		Figure 21-85
Video	iMG_Video_shared_voice		Figure 21-86
Voice	iMG_voice_shared_video		Figure 21-87



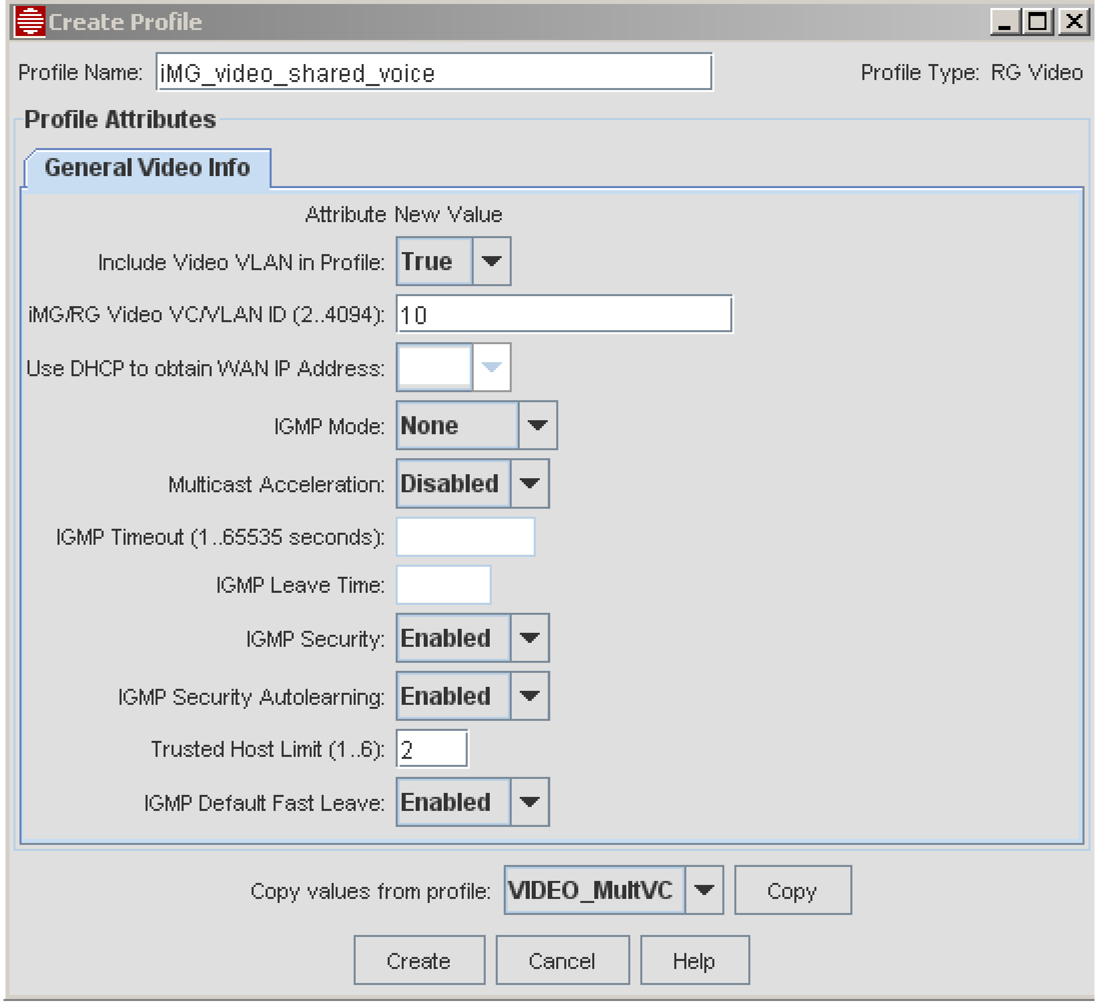
Profile Name: iMG_Data_only_VLAN20

Profile Type: RG Internet

Internet Service Type:	Routed Service
Include Internet VLAN in Profile:	True
iMG/RG Internet VC/VLAN Id (2..4094):	20
Use PPPoE:	False
iMG/RG Local Customer VLAN Id (2..4094):	2
Use DHCP to obtain WAN IP Address:	False
DNS Servers (list of IP Addrs. or None):	None
Local IP Address:	
Local Mask:	
Local DHCP Start IP Address:	
Local DHCP End IP Address:	
Rate Limiting:	Disabled
Up. Rate Limit (1..50000 kbps):	
Up. Burst Size (1..67108 bps):	
Up. Scalar (1..100):	
Down. Rate Limit (1..50000 kbps):	
Down. Burst Size (1..67108 bps):	
Down. Scalar (1..100):	

Copy values from profile: iMG_data_shared_VLAN_video

FIGURE 21-85 Internet Form for Multi-service VLAN General Internet Info Tab - Configuration 2



Profile Name: iMG_video_shared_voice

Profile Type: RG Video

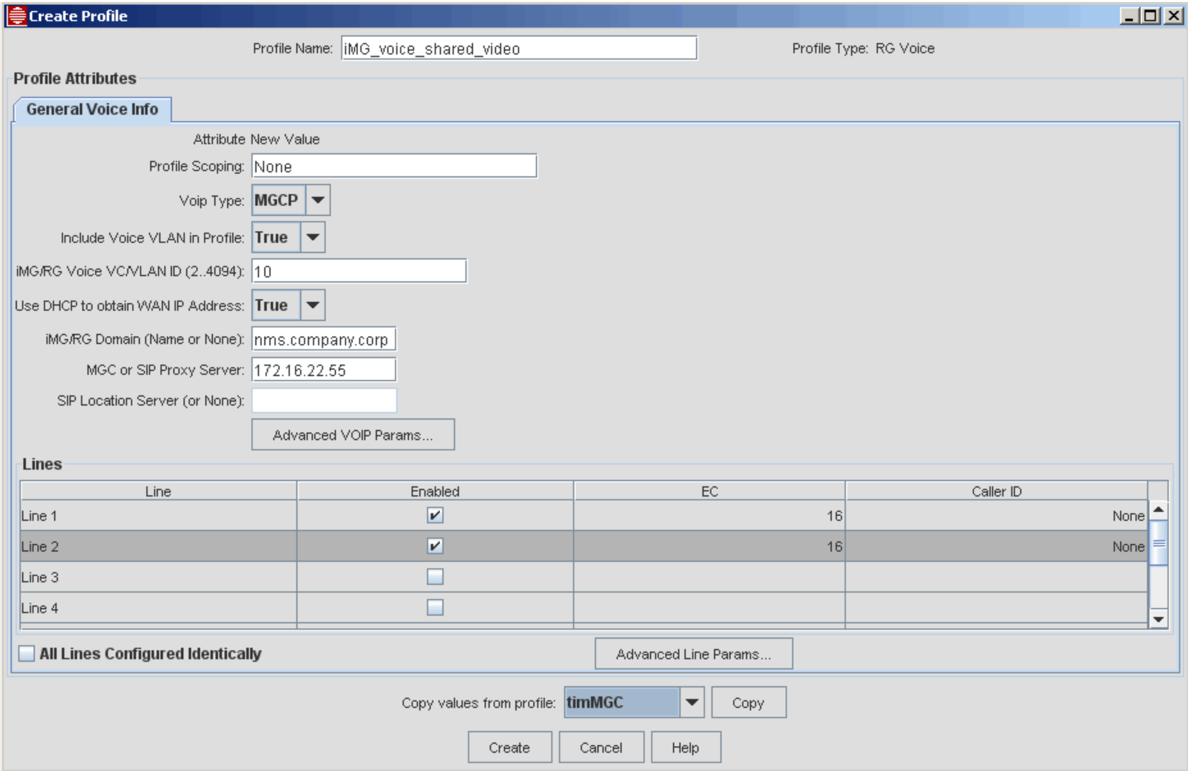
Profile Attributes

General Video Info

Attribute	New Value
Include Video VLAN in Profile:	True
iMG/RG Video VC/VLAN ID (2..4094):	10
Use DHCP to obtain WAN IP Address:	
IGMP Mode:	None
Multicast Acceleration:	Disabled
IGMP Timeout (1..65535 seconds):	
IGMP Leave Time:	
IGMP Security:	Enabled
IGMP Security Autolearning:	Enabled
Trusted Host Limit (1..6):	2
IGMP Default Fast Leave:	Enabled

Copy values from profile: VIDEO_MultVC

FIGURE 21-86 Video Form for Multi-service VLAN - Configuration 2



Create Profile

Profile Name: iMG_voice_shared_video

Profile Type: RG Voice

Profile Attributes

General Voice Info

Attribute	New Value
Profile Scoping:	None
Voip Type:	MGCP
Include Voice VLAN in Profile:	True
iMG/RG Voice VC/VLAN ID (2..4094):	10
Use DHCP to obtain WAN IP Address:	True
iMG/RG Domain (Name or None):	nms.company.corp
MGC or SIP Proxy Server:	172.16.22.55
SIP Location Server (or None):	

Lines

Line	Enabled	EC	Caller ID
Line 1	☑	16	None
Line 2	☑	16	None
Line 3	□		
Line 4	□		

□ All Lines Configured Identically

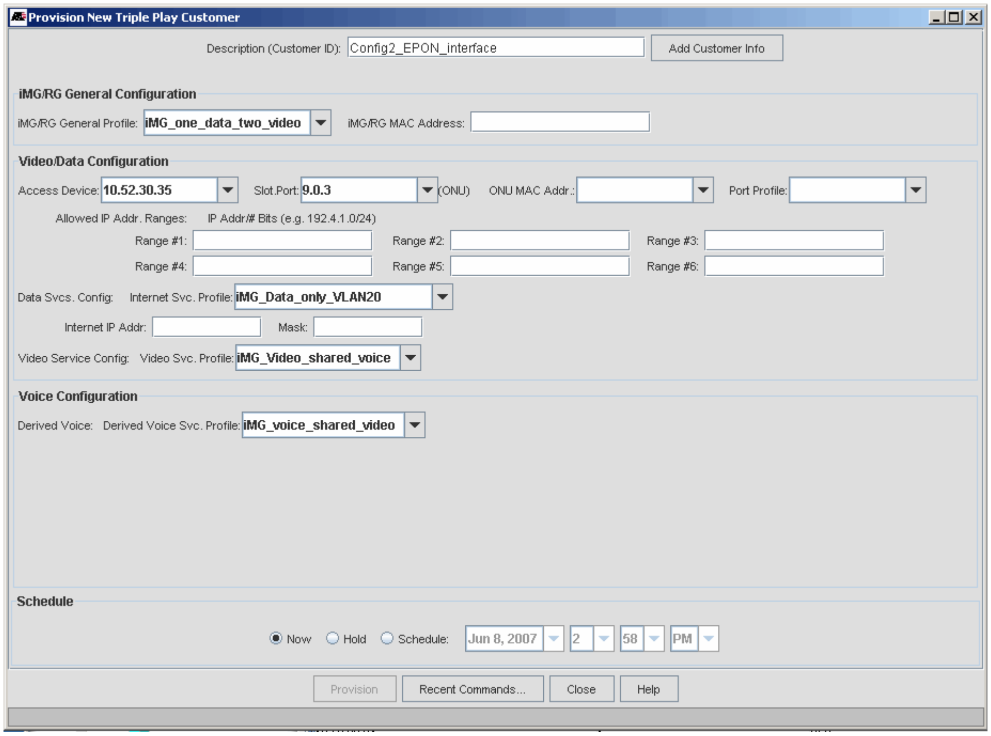
Copy values from profile: timMGC

FIGURE 21-87 Voice Form for Multi-service VLAN - Configuration 2

2. Data fill the Triple-Play Form. Since there are three different customers and types of interfaces, the Customer ID for each must be unique, and the slot.Port will be different. (The iMAP could be the same if all of the interface cards were on the same iMAP. Refer to the following table.)

TABLE 21-11 Triple Play Forms for Voice, Video/Data VLAN Configuration

iMG Type	Attributes	Reference
EPON (iMG646PX-ON)		Figure 21-88
FX (iMG646)		Figure 21-89
ADSL (iMG634)		Figure 21-90



Provision New Triple Play Customer

Description (Customer ID): Config2_EPON_interface

iMG/RG General Configuration

iMG/RG General Profile: iMG_one_data_two_video

iMG/RG MAC Address:

Video/Data Configuration

Access Device: 10.52.30.35

Slot.Port: 9.0.3 (ONU)

ONU MAC Addr.:

Port Profile:

Allowed IP Addr. Ranges: IP Addr/# Bits (e.g. 192.4.1.0/24)

Range #1: Range #2: Range #3:

Range #4: Range #5: Range #6:

Data Svcs. Config: Internet Svc. Profile: iMG_Data_only_VLAN20

Internet IP Addr: Mask:

Video Service Config: Video Svc. Profile: iMG_Video_shared_voice

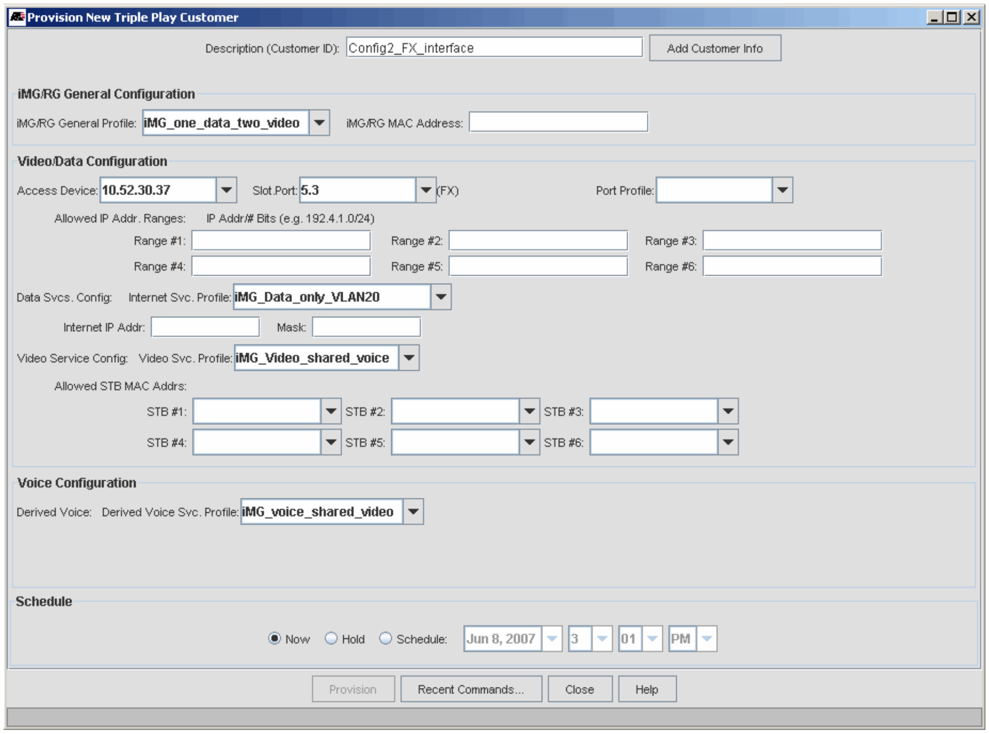
Voice Configuration

Derived Voice: Derived Voice Svc. Profile: iMG_voice_shared_video

Schedule

● Now ○ Hold ○ Schedule: Jun 8, 2007 2 58 PM

FIGURE 21-88 Triple-Play Form EPON Interface - Configuration 2



Provision New Triple Play Customer

Description (Customer ID): Config2_FX_interface

iMG/RG General Configuration

iMG/RG General Profile: iMG_one_data_two_video

iMG/RG MAC Address:

Video/Data Configuration

Access Device: 10.52.30.37

Slot.Port: 5.3 (FX)

Port Profile:

Allowed IP Addr. Ranges: IP Addr/# Bits (e.g. 192.4.1.0/24)

Range #1: Range #2: Range #3:

Range #4: Range #5: Range #6:

Data Svcs. Config: Internet Svc. Profile: iMG_Data_only_VLAN20

Internet IP Addr: Mask:

Video Service Config: Video Svc. Profile: iMG_Video_shared_voice

Allowed STB MAC Addrs:

STB #1: STB #2: STB #3:

STB #4: STB #5: STB #6:

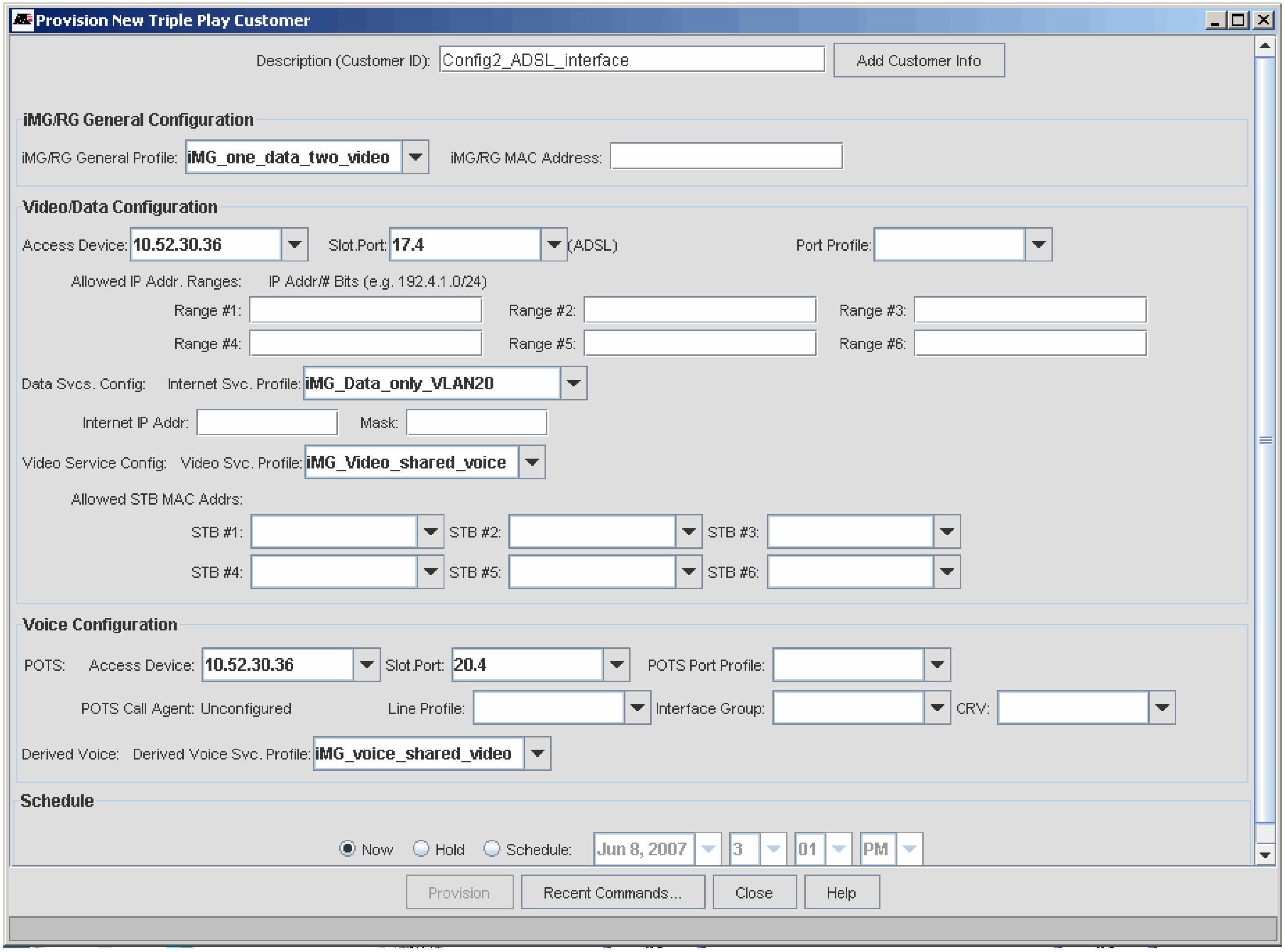
Voice Configuration

Derived Voice: Derived Voice Svc. Profile: iMG_voice_shared_video

Schedule

● Now ○ Hold ○ Schedule: Jun 8, 2007 3 01 PM

FIGURE 21-89 Triple-Play Form FX Interface - Configuration 2



Description (Customer ID): Config2_ADSL_interface

iMG/RG General Configuration

iMG/RG General Profile: iMG_one_data_two_video

iMG/RG MAC Address:

Video/Data Configuration

Access Device: 10.52.30.36

Slot.Port: 17.4 (ADSL)

Port Profile:

Allowed IP Addr. Ranges: IP Addr/# Bits (e.g. 192.4.1.0/24)

Range #1: Range #2: Range #3:

Range #4: Range #5: Range #6:

Data Svcs. Config: Internet Svc. Profile: iMG_Data_only_VLAN20

Internet IP Addr: Mask:

Video Service Config: Video Svc. Profile: iMG_Video_shared_voice

Allowed STB MAC Addrs:

STB #1: STB #2: STB #3:

STB #4: STB #5: STB #6:

Voice Configuration

POTS: Access Device: 10.52.30.36 Slot.Port: 20.4 POTS Port Profile:

POTS Call Agent: Unconfigured Line Profile: Interface Group: CRV:

Derived Voice: Derived Voice Svc. Profile: iMG_voice_shared_video

Schedule

● Now ○ Hold ○ Schedule: Jun 8, 2007 3 01 PM

FIGURE 21-90 Triple-Play Form ADSL Interface - Configuration 2

21.15.11.3 Creating a Video and Data/Voice VLAN (Configuration 3)

In this configuration, the Video VLAN is a separate VLAN, and data and voice share a single VLAN. Refer to the following figure and notes in Configuring multi-service VLAN before performing the procedure.

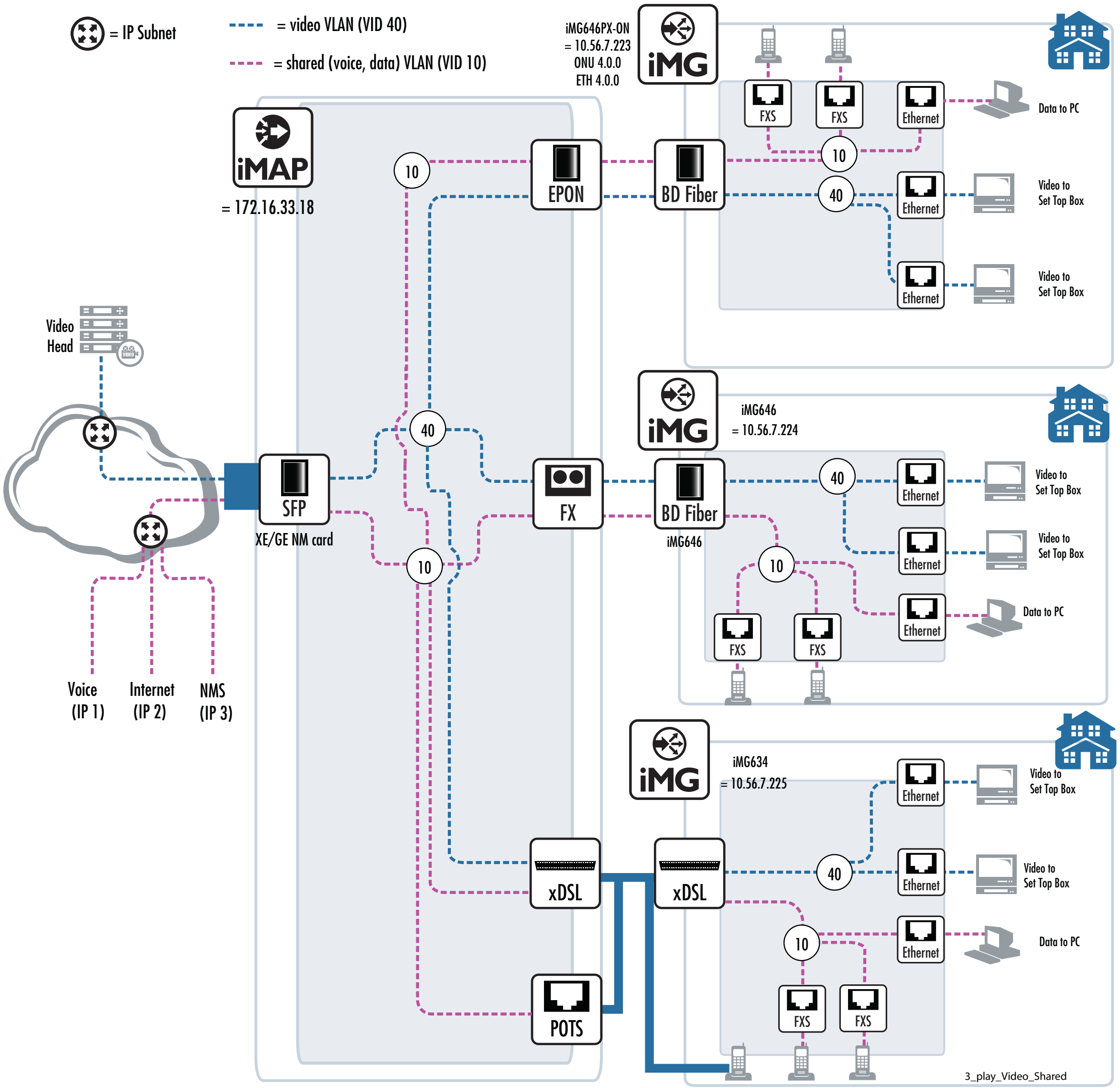
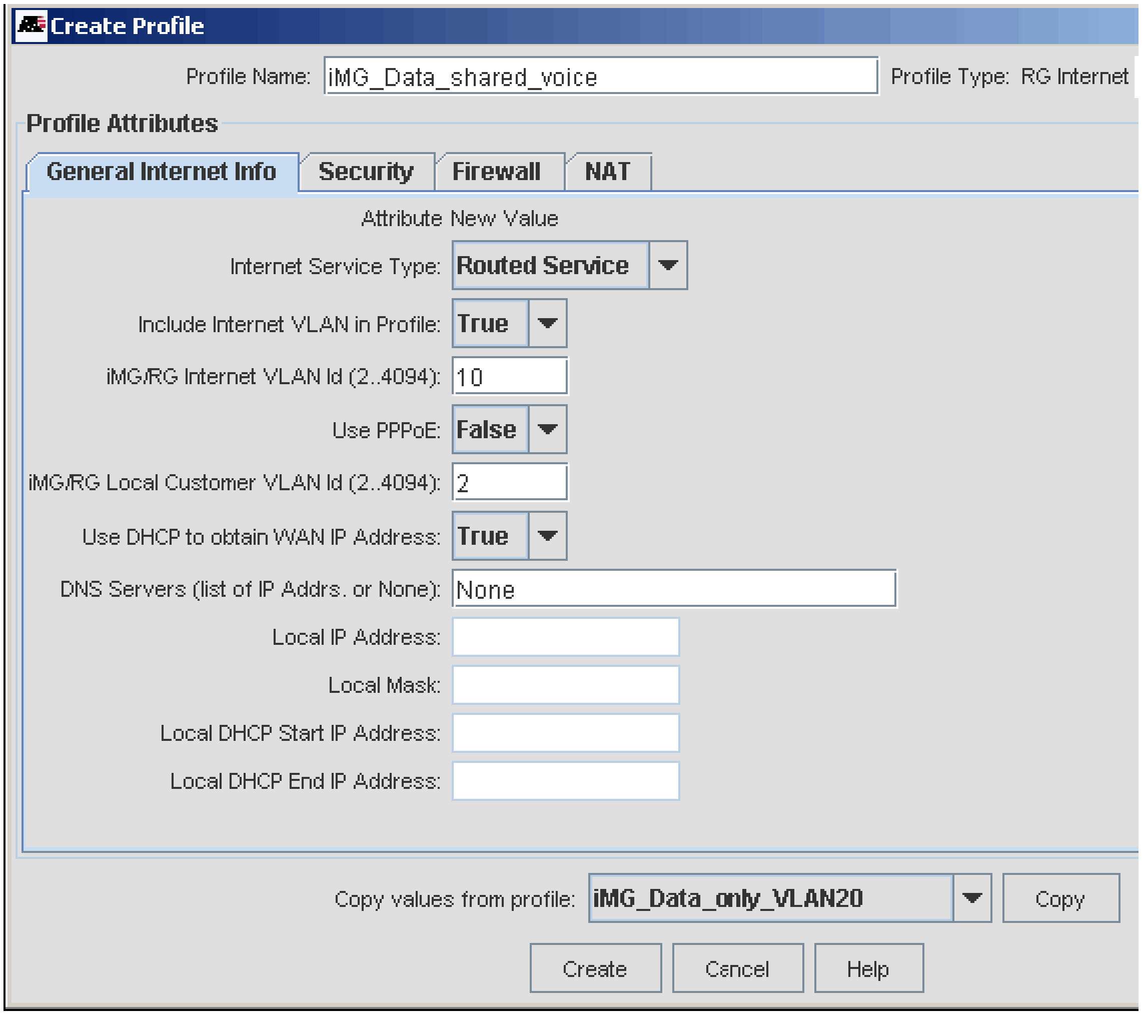


FIGURE 21-91 Multi-service (Data, Voice) VLAN (Configuration 3)

1. Create the appropriate iMG profiles. Refer to the following table and figures.

TABLE 21-12 iMG Forms for Voice, Video/Data VLAN (Configuration) 2

Form	Name	Attributes	Reference
General	iMG_one_data_two_video	SInce the port and VLAN configuration is the same for all iMGs, the same General Form is used in all configurations	Figure 21-76 - Mgmt. Info Figure 21-77 - Port Assignment
Internet	iMG_Data_shared_voice		Figure 21-85
Video	iMG_Video_VLAN_40		Figure 21-86
Voice	iMG_Voice_shared_data		Figure 21-87



Create Profile

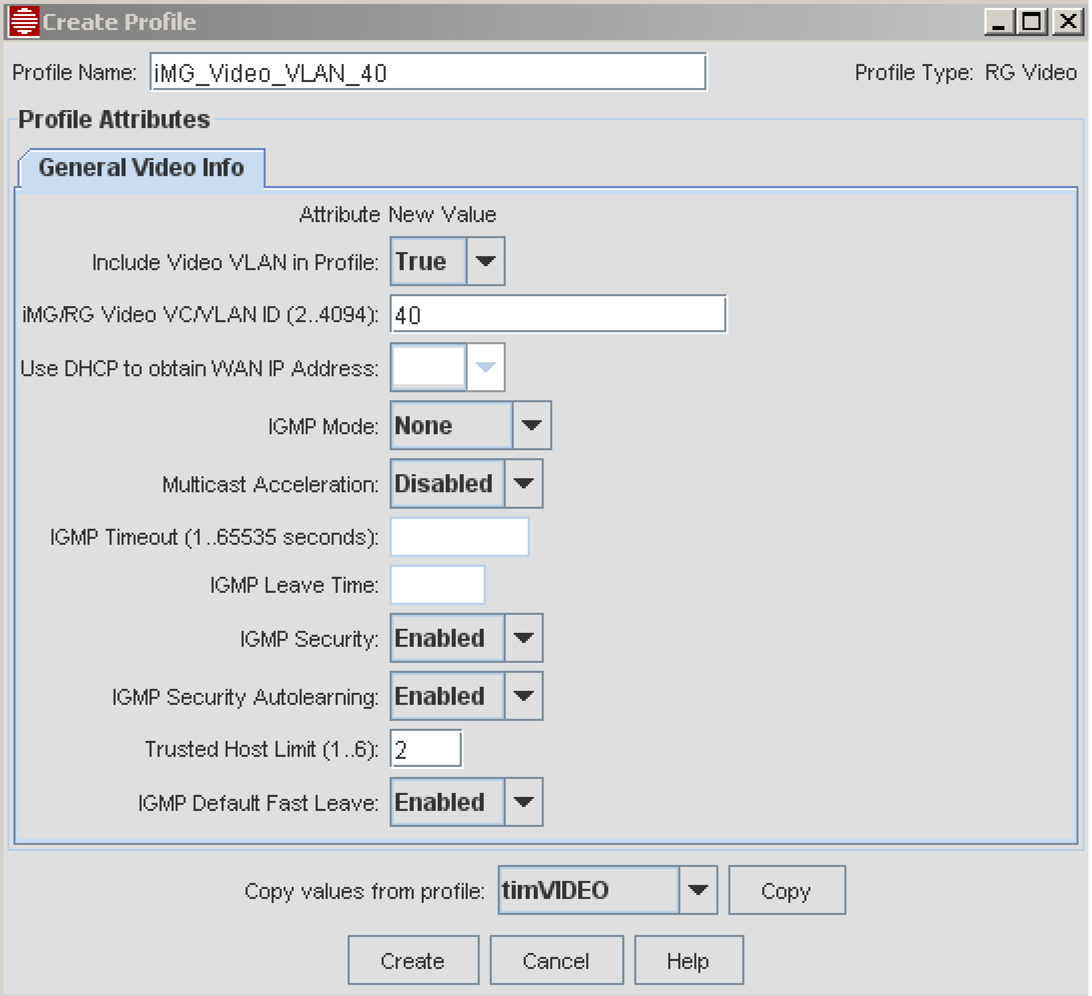
Profile Name: iMG_Data_shared_voice Profile Type: RG Internet

Profile Attributes

Attribute	New Value
Internet Service Type:	Routed Service
Include Internet VLAN in Profile:	True
iMG/RG Internet VLAN Id (2..4094):	10
Use PPPoE:	False
iMG/RG Local Customer VLAN Id (2..4094):	2
Use DHCP to obtain WAN IP Address:	True
DNS Servers (list of IP Addrs. or None):	None
Local IP Address:	
Local Mask:	
Local DHCP Start IP Address:	
Local DHCP End IP Address:	

Copy values from profile: iMG_Data_only_VLAN20

FIGURE 21-92 Internet Form for Multi-service VLAN General Internet Info Tab - Configuration 3

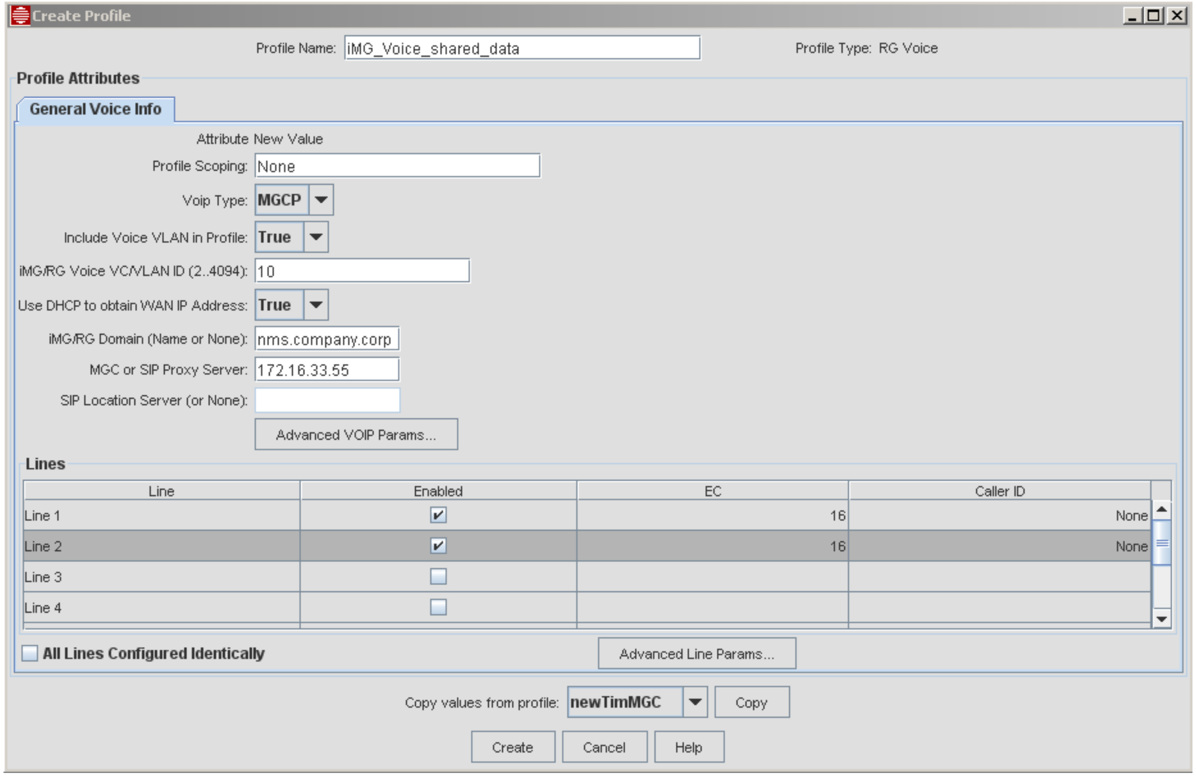


Profile Name:	iMG_Video_VLAN_40
Profile Type:	RG Video

Attribute	New Value
Include Video VLAN in Profile:	True
iMG/RG Video VC/VLAN ID (2..4094):	40
Use DHCP to obtain WAN IP Address:	
IGMP Mode:	None
Multicast Acceleration:	Disabled
IGMP Timeout (1..65535 seconds):	
IGMP Leave Time:	
IGMP Security:	Enabled
IGMP Security Autolearning:	Enabled
Trusted Host Limit (1..6):	2
IGMP Default Fast Leave:	Enabled

Copy values from profile: timVIDEO

FIGURE 21-93 Video Form for Multi-service VLAN - Configuration 3



Profile Name: iMG_Voice_shared_data
Profile Type: RG Voice

Attribute New Value

Profile Scoping: None

Voip Type: MGCP

Include Voice VLAN in Profile: True

iMG/RG Voice VC/VLAN ID (2..4094): 10

Use DHCP to obtain WAN IP Address: True

iMG/RG Domain (Name or None): nms.company.corp

MGC or SIP Proxy Server: 172.16.33.55

SIP Location Server (or None):

Line	Enabled	EC	Caller ID
Line 1	☑	16	None
Line 2	☑	16	None
Line 3	□		
Line 4	□		

□ All Lines Configured Identically

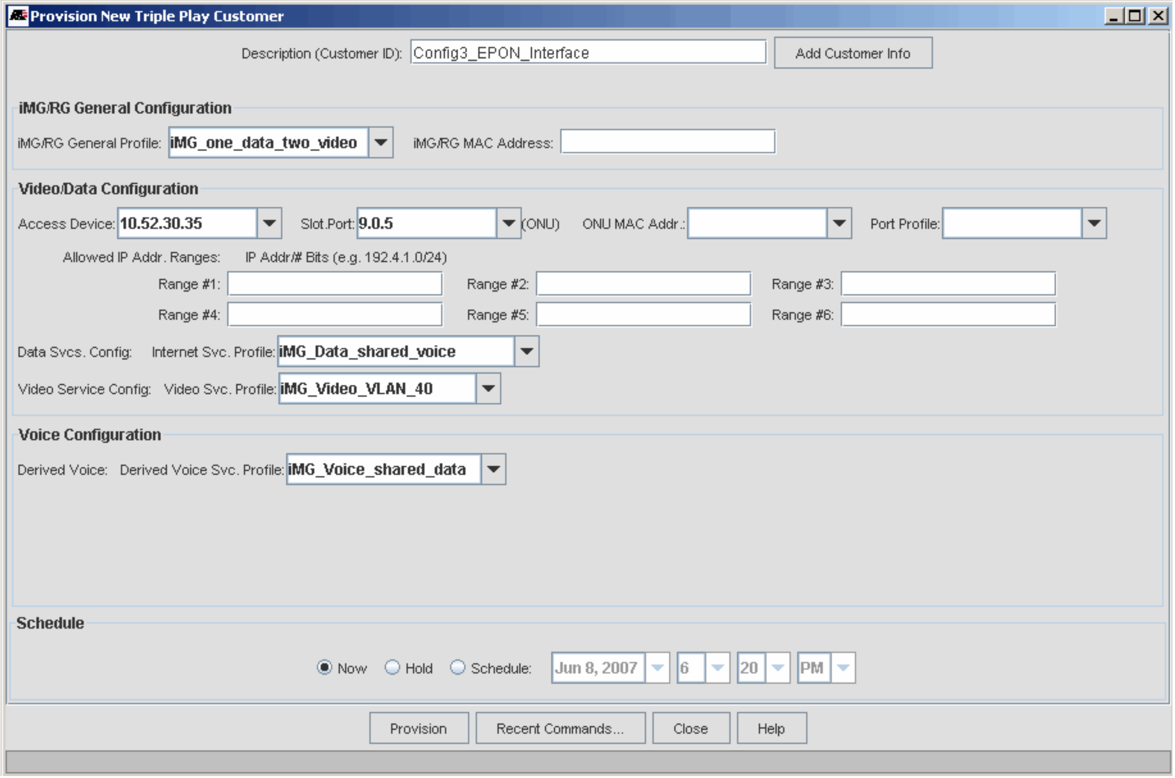
Copy values from profile: newTimMGC

FIGURE 21-94 Voice Form for Multi-service VLAN - Configuration 3

2. Data fill the Triple-Play Form. Since there are three different customers and types of interfaces, the Customer ID for each must be unique, and the slot.Port will be different. (The iMAP could be the same if all of the interface cards were on the same iMAP. Refer to the following table.

TABLE 21-13 Triple Play Forms for Voice, Video/Data VLAN Configuration

iMG Type	Attributes	Reference
EPON (iMG646PX-ON		Figure 21-95
FX (iMG646)		Figure 21-96
ADSL (iMG634)		Figure 21-97



Provision New Triple Play Customer

Description (Customer ID): Config3_EPON_Interface

iMG/RG General Configuration

iMG/RG General Profile: iMG_one_data_two_video

iMG/RG MAC Address:

Video/Data Configuration

Access Device: 10.52.30.35

Slot.Port: 9.0.5 (ONU)

ONU MAC Addr.:

Port Profile:

Allowed IP Addr. Ranges: IP Addr/# Bits (e.g. 192.4.1.0/24)

Range #1: Range #2: Range #3:

Range #4: Range #5: Range #6:

Data Svcs. Config: Internet Svc. Profile: iMG_Data_shared_voice

Video Service Config: Video Svc. Profile: iMG_Video_VLAN_40

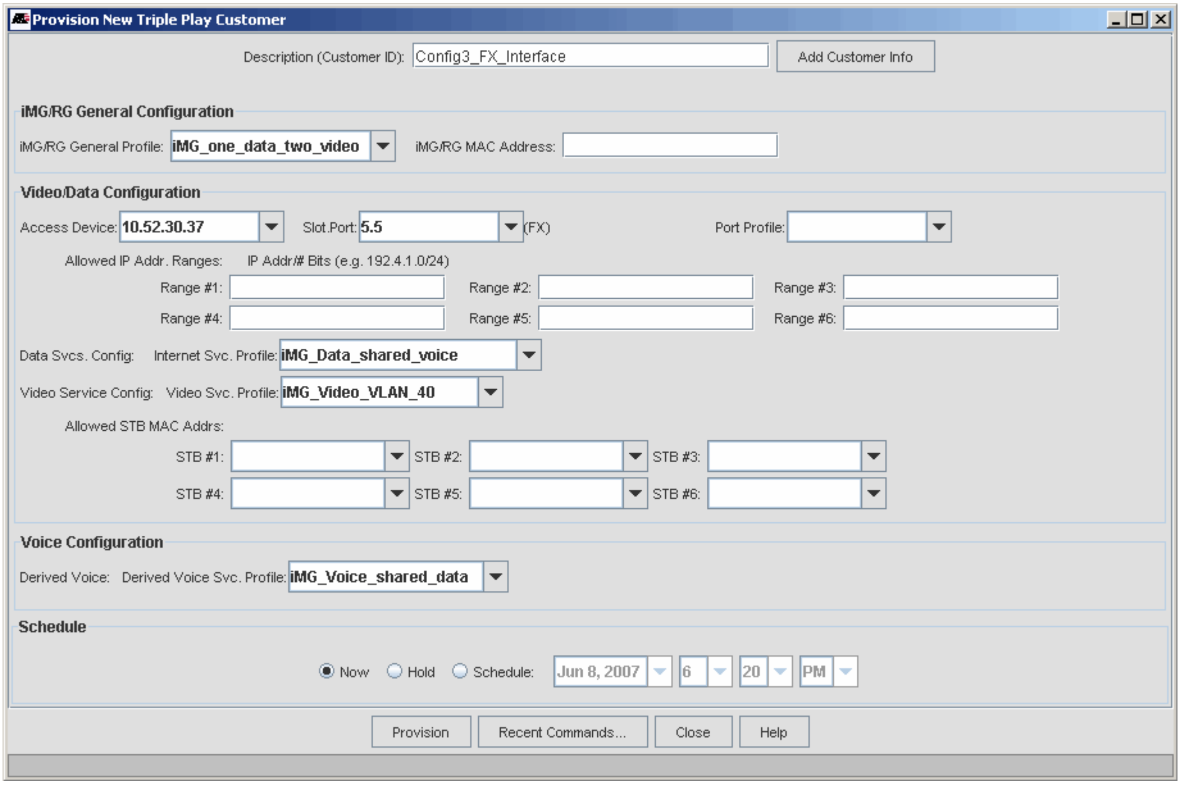
Voice Configuration

Derived Voice: Derived Voice Svc. Profile: iMG_Voice_shared_data

Schedule

● Now ○ Hold ○ Schedule: Jun 8, 2007 6 20 PM

FIGURE 21-95 Triple-Play Form EPON Interface - Configuration 2



Provision New Triple Play Customer

Description (Customer ID): Config3_FX_Interface

iMG/RG General Configuration

iMG/RG General Profile: iMG_one_data_two_video

iMG/RG MAC Address:

Video/Data Configuration

Access Device: 10.52.30.37

Slot.Port: 5.5 (FX)

Port Profile:

Allowed IP Addr. Ranges: IP Addr/# Bits (e.g. 192.4.1.0/24)

Range #1: Range #2: Range #3:

Range #4: Range #5: Range #6:

Data Svcs. Config: Internet Svc. Profile: iMG_Data_shared_voice

Video Service Config: Video Svc. Profile: iMG_Video_VLAN_40

Allowed STB MAC Addrs:

STB #1: STB #2: STB #3:

STB #4: STB #5: STB #6:

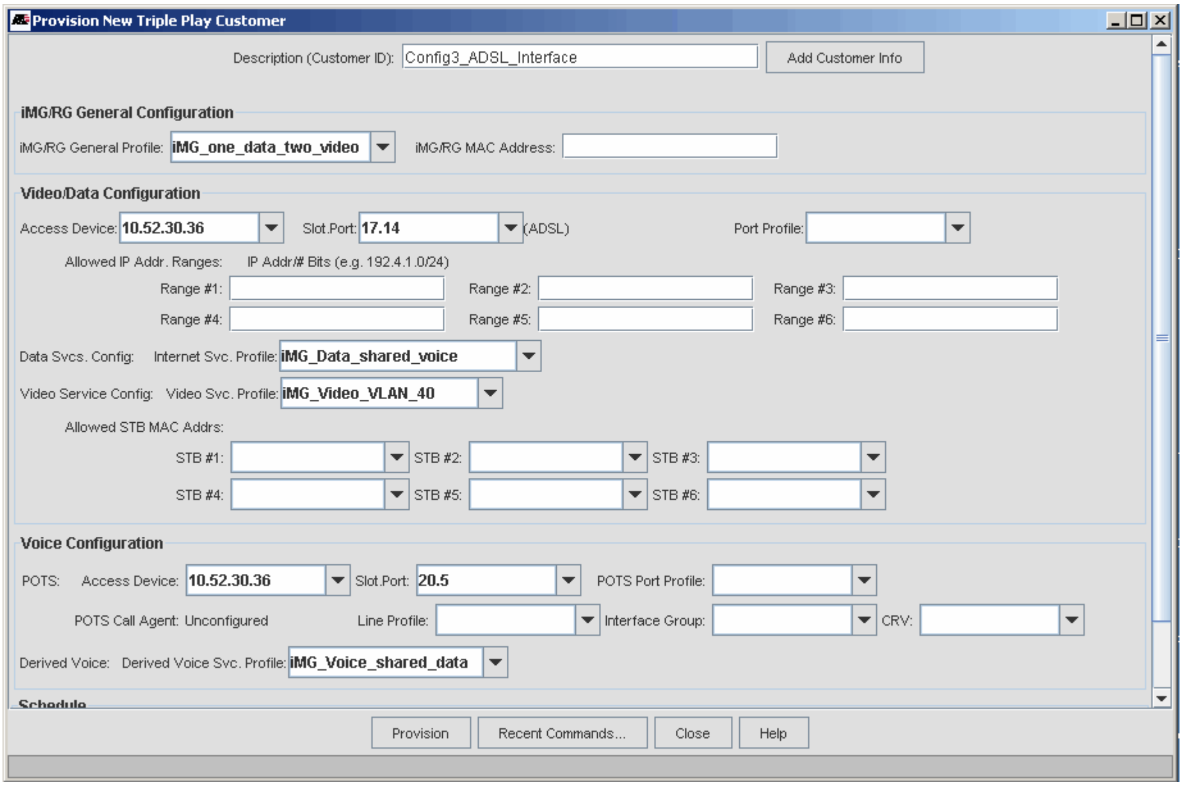
Voice Configuration

Derived Voice: Derived Voice Svc. Profile: iMG_Voice_shared_data

Schedule

● Now ○ Hold ○ Schedule: Jun 8, 2007 6 20 PM

FIGURE 21-96 Triple-Play Form FX Interface - Configuration 3



Description (Customer ID): Config3_ADSL_Interface

iMG/RG General Profile: iMG_one_data_two_video
iMG/RG MAC Address:

Access Device: 10.52.30.36
Slot.Port: 17.14 (ADSL)
Port Profile:

Allowed IP Addr. Ranges: IP Addr/# Bits (e.g. 192.4.1.0/24)
Range #1: Range #2: Range #3:
Range #4: Range #5: Range #6:

Data Svcs. Config: Internet Svc. Profile: iMG_Data_shared_voice

Video Service Config: Video Svc. Profile: iMG_Video_VLAN_40

Allowed STB MAC Addrs:
STB #1: STB #2: STB #3:
STB #4: STB #5: STB #6:

POTS: Access Device: 10.52.30.36 Slot.Port: 20.5 POTS Port Profile:

POTS Call Agent: Unconfigured Line Profile: Interface Group: CRV:

Derived Voice: Derived Voice Svc. Profile: iMG_Voice_shared_data

FIGURE 21-97 Triple-Play Form ADSL Interface - Configuration 3

21.16 Provisioning the iMG (no iMAP or AW+)

Note: Section Configuration 8 - AlliedWare Plus Device provides an overview of provisioning the iMG/RG on AlliedWare Plus (AW+) devices, and how it has the same feature coordination as with iMAPs.

When both the iMG and upstream port are controlled by the NMS, you can coordinate certain provisioning features to provision, query, and control one or more iMGs quickly and efficiently.

An iMG attached to a device other than an iMAP or AW+ device can still be provisioned with the NMS. If the correct steps are taken, the NMS can provision the iMG so that it provides all of its supported services.

When an iMAP and its attributes are not included and are therefore not part of a provisioning/maintaining scenario, the following concepts are altered or not applicable:

- Port Profiles are not part of provisioning.
- DNS Entries for iMAPs (remote IDs) are not included. This is what controls the next item.
- Scoping in the iMG profiles is not part of provisioning.
- The Customer ID applies only to the iMG/RG (and optionally to GenBand).
- In the Triple Play Provisioning window, preferences should be set so that iMAP-related fields do not appear or are masked out.
- Only statistics related to the iMG/RG are displayed in the Triple Play Management window.
- DHCP is still used for provisioning, but the set-up and steps followed are different.
- Since there are no iMAPs in this scenario, the administrator is responsible for all network connections between the iMG/RG, DHCP server, NMS, and service providers. (The network is shown as only a cloud rather than a cloud that includes iMAP interfaces and specific service providers.)

These concepts are explained below.

21.16.1 DHCP Provisioning

21.16.1.1 iMGs/RGs at Release 3-x

As explained in Configuring Components for DHCP Discovery, the iMG/RG, DHCP server, and AlliedView NMS use DHCP to provide provisioning information and to download files until the iMG/RG and its network connections are recognized so that services can be supported. This is still done, as shown in Figure 21-98, but the following is changed.

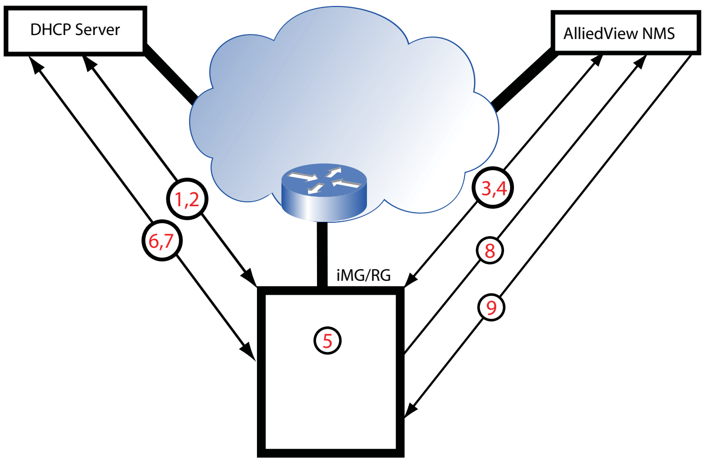
- Provisioning is tied to the MAC address of the iMG/RG, and must be known before provisioning.
- At the NMS, the RGbootConfigurator must be filled out with TFTP Discovery **Enabled**. When selected, after the RG reboots it sends a DHCP discovery message to the DHCP server (over the RGMgmt VLAN). The iMG/RG then sends a tftp request to the NMS, containing its MAC and IP address. The NMS uses its tftp listener to discover the iMG/RG with this MAC and IP Address. With the IP and MAC Address, the AlliedView NMS can proceed with discovery and provisioning.

Note: *With the iMG/RG provisioned with a specific MAC address, the iMG/RG cannot simply be swapped with another one when performing provisioning or maintenance and having the NMS automatically provision the new iMG/RG. At the NMS, the administrator must delete all objects or traces so that the iMG is no longer known to the NMS. You would then start provisioning from the beginning, by knowing the MAC address of the new iMG.*

- The dhcpd.conf file must include the NMS IP address.

Refer to Figure 21-98, which shows the steps that are followed

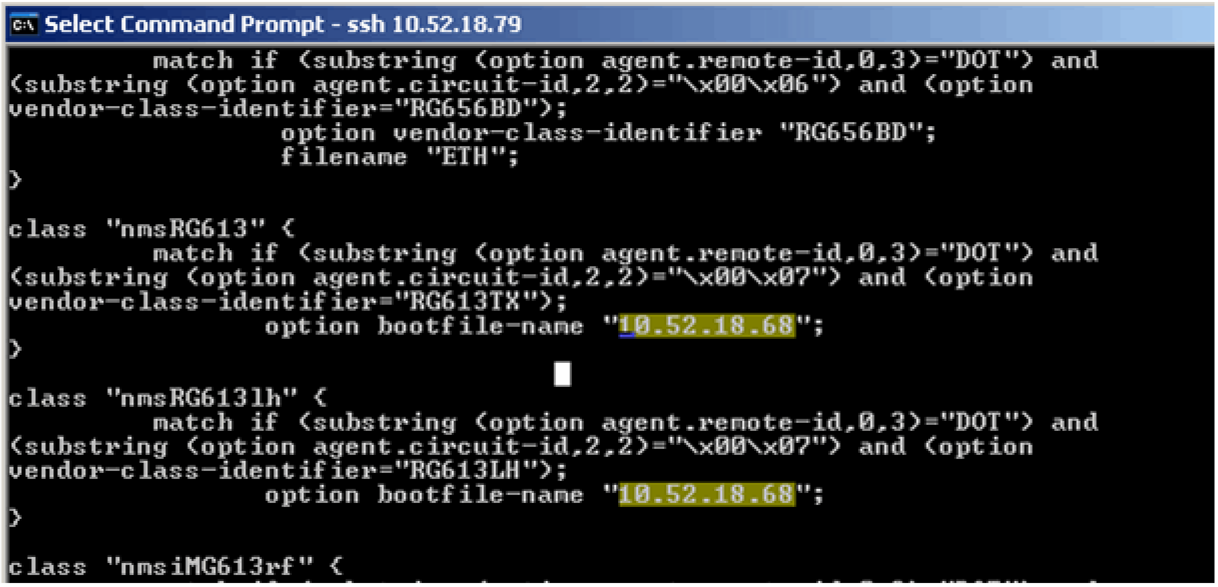
Pre-provision:
- Fill out MAC Address of the iMG/RG on the Triple Play form
- RGbootConfigurator set up with Download file with TFTP Enable
- dhcpd.conf has NMS IP Address



Step 1 iMG/RG request for Boot IP Address and TFTP Server IP Address
Step 2 DHCP Server returns information
Step 3,4 iMG/RG downloads new software and base config file (includes ZTC Enabled and Mgmt VLAN configured)
Step 5 iMG/RG reboots using new configuration
Step 6 iMG/RG requests Mgmt IP Address and NMS IP Address (=ZTC Server Address) from DHCP Server
Step 7 DHCP Server returns information
Step 8 iMG/RG sends ZTC-like TFTP request to NMS (includes IP and MAC address)
Step 9 NMS has IP/MAC Address mapping, begins provisioning

FIGURE 21-98 DHCP Provisioning for iMG/RG without an iMAP Interface

Figure 21-99 shows an example from a dhcpd.conf file. The option bootfile-name points to NMS IP address, to which the iMG/RG will send a tftp request.



Select Command Prompt - ssh 10.52.18.79

```
         match if (substring (option agent.remote-id,0,3)="DOT") and
(substring (option agent.circuit-id,2,2)="\x00\x06") and (option
vendor-class-identifier="RG656BD");
                 option vendor-class-identifier "RG656BD";
                 filename "ETH";
}

class "nmsRG613" {
         match if (substring (option agent.remote-id,0,3)="DOT") and
(substring (option agent.circuit-id,2,2)="\x00\x07") and (option
vendor-class-identifier="RG613TX");
                option bootfile-name "10.52.18.68";
}

class "nmsRG613lh" {
         match if (substring (option agent.remote-id,0,3)="DOT") and
(substring (option agent.circuit-id,2,2)="\x00\x07") and (option
vendor-class-identifier="RG613LH");
                option bootfile-name "10.52.18.68";
}

class "nmsiMG613rf" {
```

FIGURE 21-99 dhcpd.conf File - Snippet

21.16.1.2 iMGs/RGs at Release 4 and above

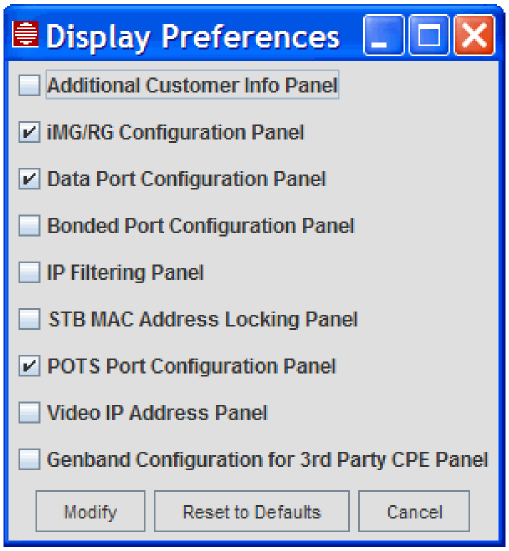
As described above, the TFTP Discovery option is used to handle customer provisioning without an iMAP or AlliedWare Plus upstream device and without forwarding DHCP Relay messages to the NMS (option 82).

The iMGs at release 4 and above do not support TFTP discovery, and so the RGbootConfigurator does not have the TFTP Discovery option (tab 4; refer to Configuring Components for DHCP Discovery). DHCP Discovery must be used, with the following rules:

- Ensure the DHCP Server File (dhcpd.conf) has the options associated with the specific VLAN in the DHCP message (refer to DHCP Server File (dhcpd.conf)).
- The upstream devices must be configured to forward DHCP Relay messages to the NMS when it gives out RgMgmt IPs as in section DHCP Server File (dhcpd.conf).
- Use the vendor-specific option 82 value to define separate classes for the Boot and Mgmt VLANs.
- Configure the Boot class as in section DHCP Server File (dhcpd.conf).
- Configure the DHCP Mgmt class as in section DHCP Server File (dhcpd.conf), that is, option bootfile-name is not required.
- Enter the iMG MAC address in the "Provision New Triple Play Customer" dialog, as shown in Figure 21-101.

21.16.2 GUI Provisioning

With the Display Preferences feature, you see only the fields that are relevant for the provisioning scenario, and fields that need to be filled in are highlighted as you fill out the fields. In the Display Preferences GUI, there is the iMG/RG Configuration Panel. When selected, the Triple Play form limits the shown fields to only those that are iMG/RG related. Refer to the following figures.



Display Preferences

☐ Additional Customer Info Panel

☑ iMG/RG Configuration Panel

☑ Data Port Configuration Panel

☐ Bonded Port Configuration Panel

☐ IP Filtering Panel

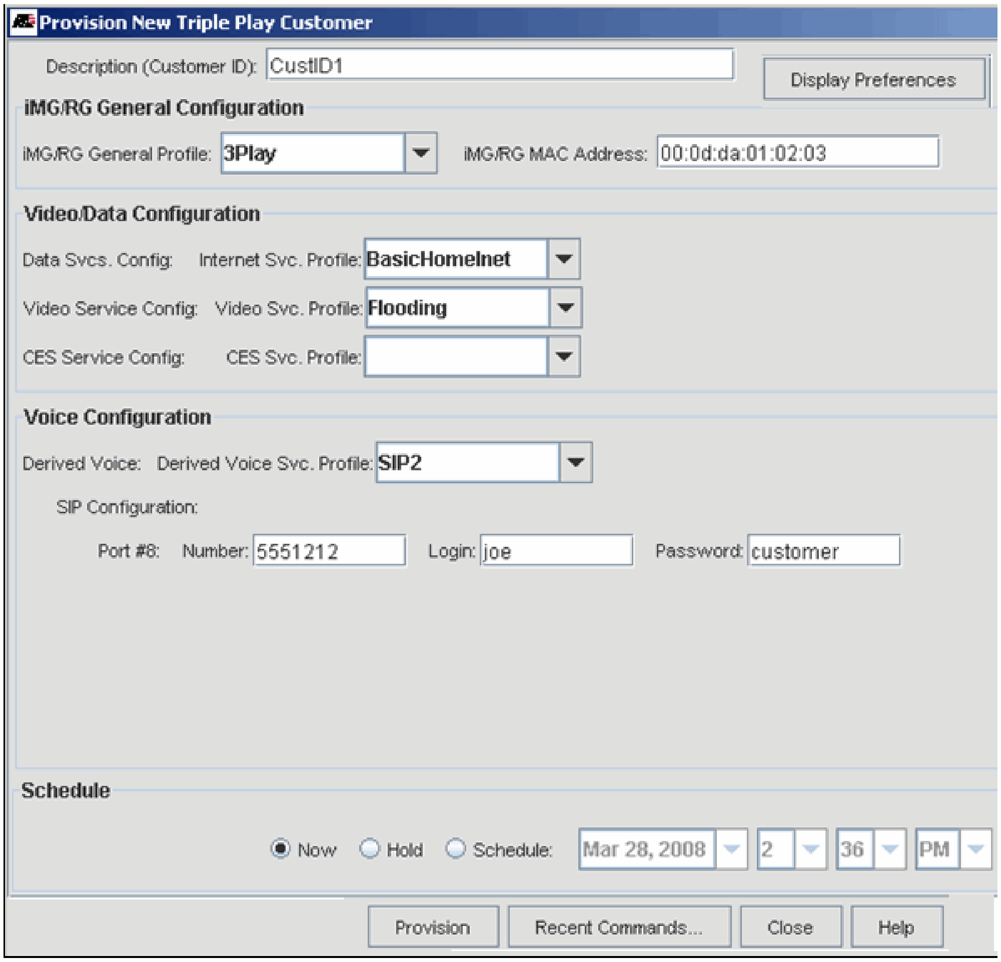
☐ STB MAC Address Locking Panel

☑ POTS Port Configuration Panel

☐ Video IP Address Panel

☐ Genband Configuration for 3rd Party CPE Panel

FIGURE 21-100 Display Preferences set for iMG/RG



Provision New Triple Play Customer

Description (Customer ID): CustID1

iMG/RG General Configuration

iMG/RG General Profile: 3Play iMG/RG MAC Address: 00:0d:da:01:02:03

Video/Data Configuration

Data Svcs. Config: Internet Svc. Profile: BasicHomeInet

Video Service Config: Video Svc. Profile: Flooding

CES Service Config: CES Svc. Profile:

Voice Configuration

Derived Voice: Derived Voice Svc. Profile: SIP2

SIP Configuration:

Port #8: Number: 5551212 Login: joe Password: customer

Schedule

● Now ○ Hold ○ Schedule: Mar 28, 2008 2 36 PM

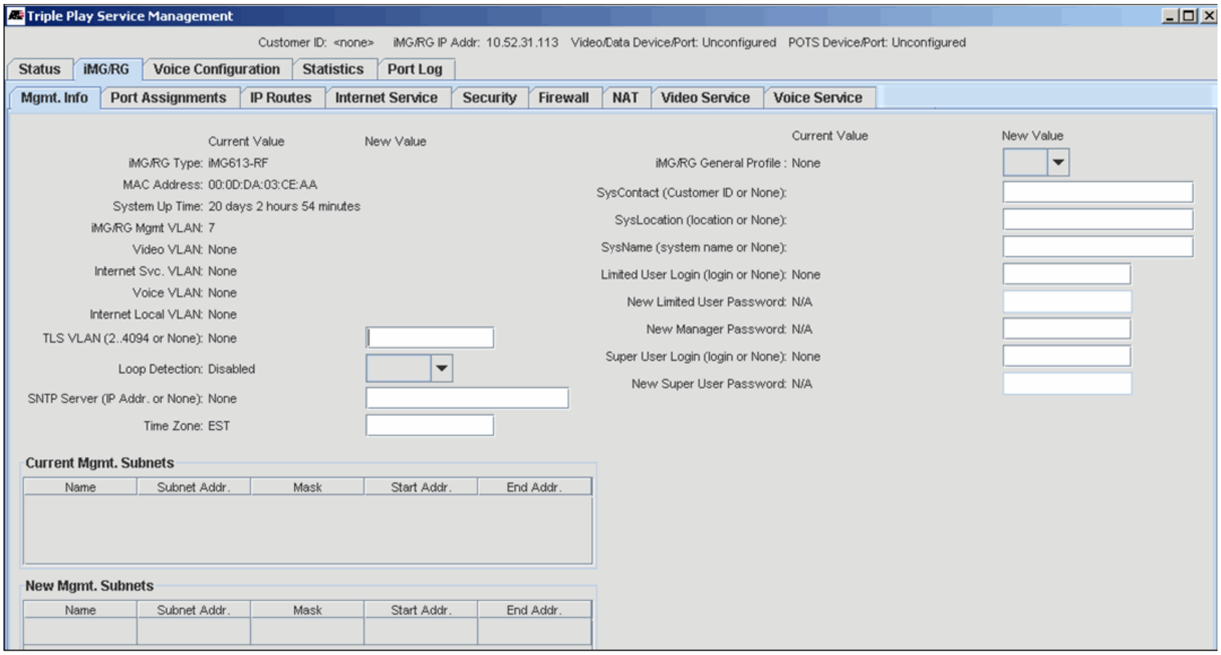
FIGURE 21-101 Triple Play Form without iMAP-related Fields

21.16.3 GUI Displays

Once the iMG is provisioned, the Details Panels are changed as follows:

- There is no Eth/ADSL tab.
- The statistics tab doesn't have PMON or RMON stats
- The graph Stats Tab only lists iMG stats

Refer to the following figure.



Customer ID: <none> iMG/RG IP Addr: 10.52.31.113 Video/Data Device/Port: Unconfigured POTS Device/Port: Unconfigured

	Current Value	New Value
iMG/RG Type:	iMG613-RF	
MAC Address:	00:0D:DA:03:CE:AA	
System Up Time:	20 days 2 hours 54 minutes	
iMG/RG Mgmt VLAN:	7	
Video VLAN:	None	
Internet Svc. VLAN:	None	
Voice VLAN:	None	
Internet Local VLAN:	None	
TLS VLAN (2..4094 or None):	None	
Loop Detection:	Disabled	
SNTP Server (IP Addr. or None):	None	
Time Zone:	EST	

	Current Value	New Value
iMG/RG General Profile :	None	
SysContact (Customer ID or None):		
SysLocation (location or None):		
SysName (system name or None):		
Limited User Login (login or None):	None	
New Limited User Password:	N/A	
New Manager Password:	N/A	
Super User Login (login or None):	None	
New Super User Password:	N/A	

Current Mgmt. Subnets

Name	Subnet Addr.	Mask	Start Addr.	End Addr.

New Mgmt. Subnets

Name	Subnet Addr.	Mask	Start Addr.	End Addr.

FIGURE 21-102 Service Details Display for iMG/RG without iMAP Interface

21.17 Using a LAN Uplink for iMGs

The NMS can manage some iMGs over a LAN interface. The LAN interface takes the place of the WAN interface for management and all services are provided over the LAN interface. When a LAN uplink is enabled the WAN interface is disabled.

iMGs that can use a LAN uplink are:

- All iMG 1000 and iMG 2000 series iMGs
- AT-iMG624A-R2
- AT-iMG634A-R2
- AT-iMG634B-R2
- AT-iMG634WA-R2
- AT-iMG634WB-R2

AT-iMG624 and AT-iMG634 series iMGs must be running release 3-7 and up.

Figure 21-103 illustrates a normal WAN configuration compared to a LAN uplink configuration.

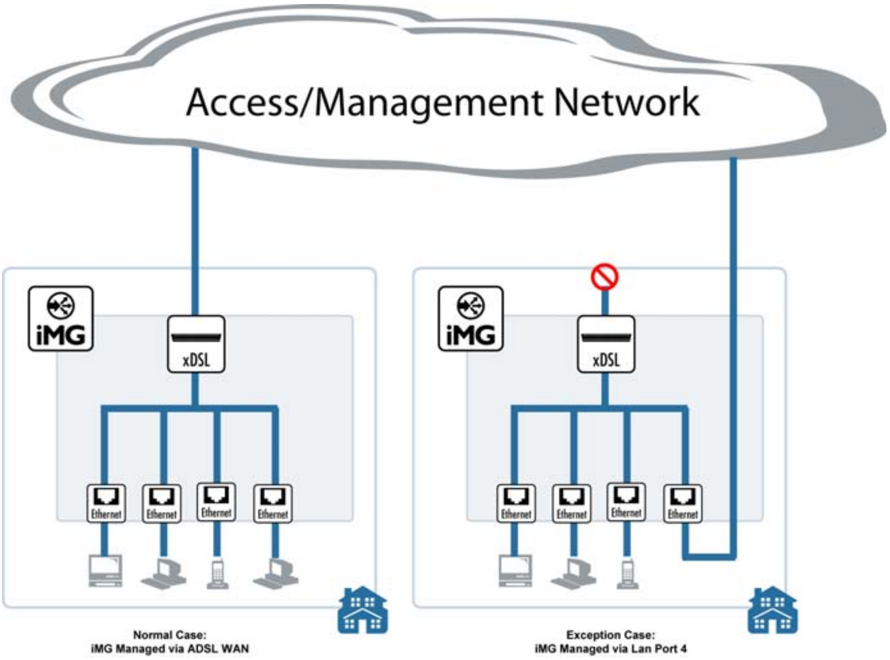


FIGURE 21-103 LAN Uplink

In a LAN uplink configuration, AT-624 and AT-634 iMGs must use the LAN 4 interface for WAN functionality. iMG 1000 and iMG 2000 series devices must use the LAN 1 interface. These interfaces are not interchangeable between the different types of iMGs.

When an iMG uses a LAN uplink, the LAN interface is no longer available for subscriber services. The NMS client identifies the LAN uplink as a management interface.

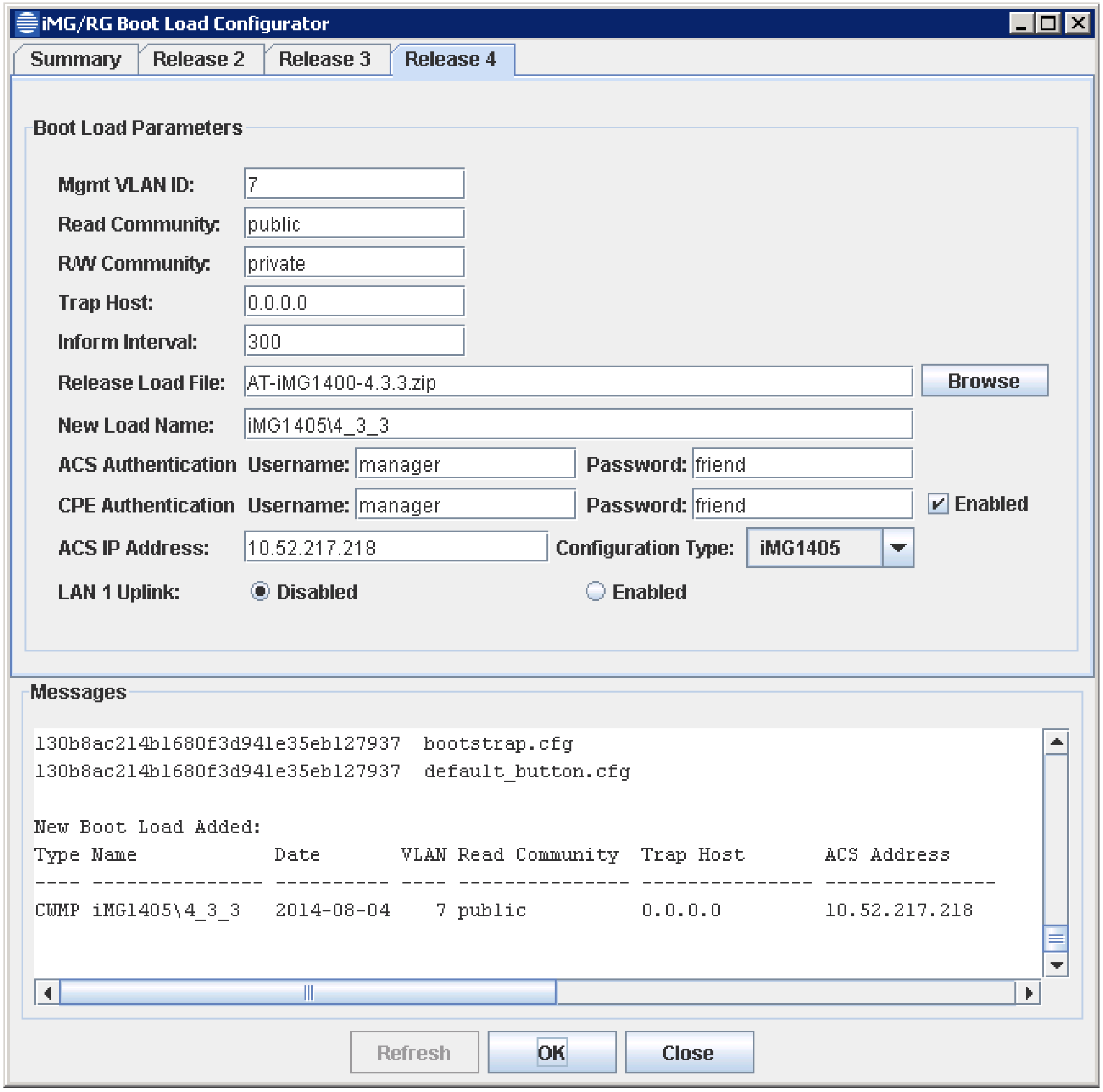
21.17.1 Setting a LAN Uplink for iMG 1000 and iMG 2000 Devices

iMG 1000 and iMG 2000 series devices use the iMG Boot Load Configurator to configure a LAN uplink.

To set a LAN uplink for an iMG 1000 or iMG 2000 device:

1. Do one of the following to launch the iMG Boot Load Configurator:
   - On Windows, go to **Start > Allied Telesis > AlliedView NMS > Tools > RG Boot Configurator**.
   - On Linux, navigate to the `<NMS_Home>/bin` directory, where `<NMS_Home>` is the directory where the NMS is installed. Run `/AT_BootConfigurator.sh`.

   The **iMG/RG Boot Load Configurator** screen appears.
2. Select the **Release 4** tab.



Boot Load Parameters

Mgmt VLAN ID: 7

Read Community: public

R/W Community: private

Trap Host: 0.0.0.0

Inform Interval: 300

Release Load File: AT-iMG1400-4.3.3.zip

New Load Name: iMG1405\4_3_3

ACS Authentication Username: manager Password: friend

CPE Authentication Username: manager Password: friend ☑ Enabled

ACS IP Address: 10.52.217.218 Configuration Type: iMG1405

LAN 1 Uplink: ● Disabled ○ Enabled

Messages

```
130b8ac214b1680f3d941e35eb127937  bootstrap.cfg
130b8ac214b1680f3d941e35eb127937  default_button.cfg

New Boot Load Added:
Type Name             Date       VLAN Read Community  Trap Host       ACS Address
---- ---------------  ---------- ---- --------------- --------------- ---------------
CWMP iMG1405\4_3_3   2014-08-04    7 public          0.0.0.0         10.52.217.218
```

FIGURE 21-104

3. Enter the **Boot Load Parameters** as required. See Table 21-4 for a description of each field.
4. Next to **LAN 1 Uplink**, select **Enabled**.
5. Click **OK** to create the boot load files.

21.17.2 Setting a LAN Uplink for AT-624 and AT-634 iMGs

AT-624 and AT-634 iMGs detect a LAN uplink automatically. When you plug an Ethernet uplink into the LAN 4 interface and the ADSL port is empty, the device is automatically configured with the LAN uplink during the boot up sequence.

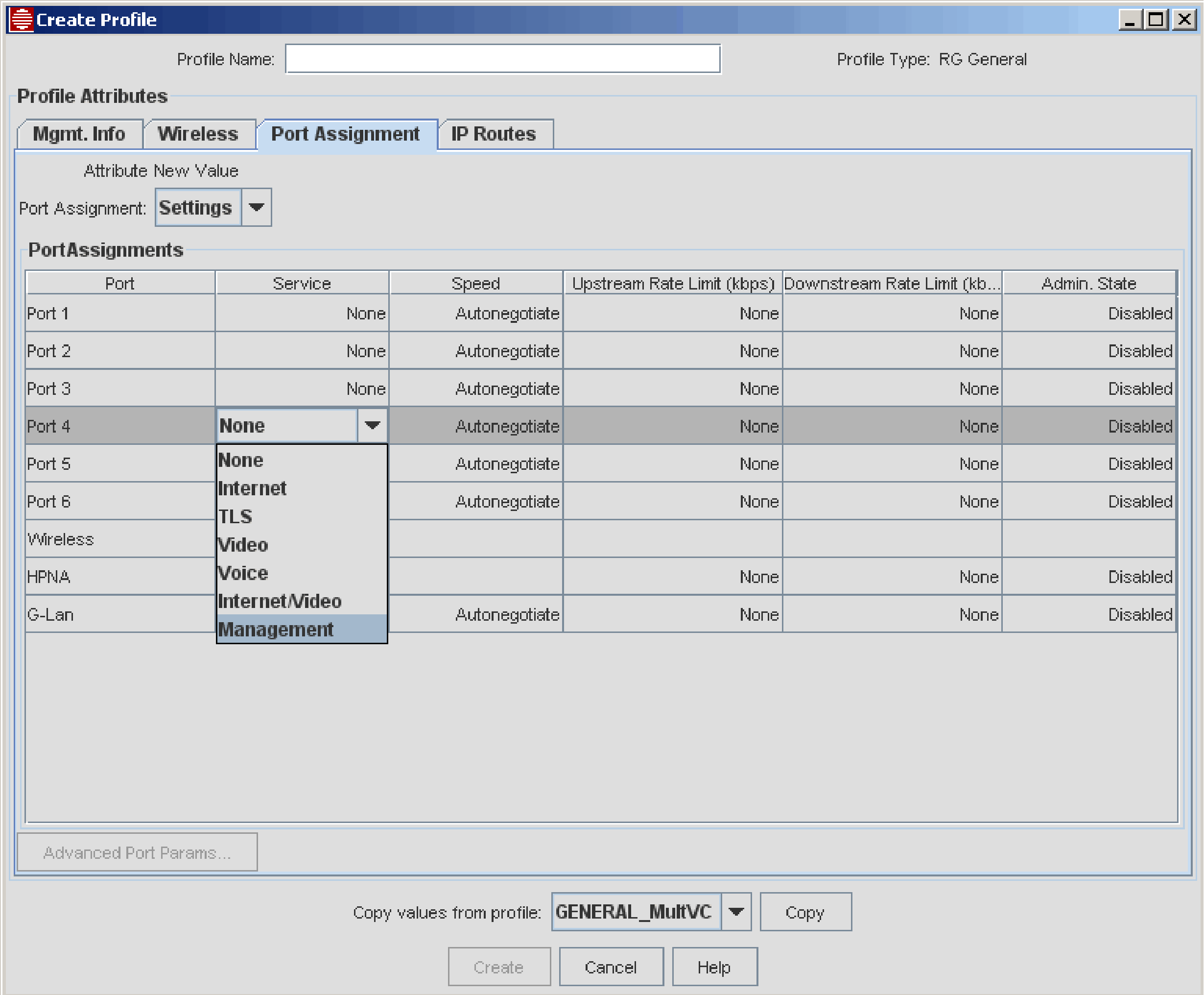
21.17.3 Creating Profiles for a LAN Uplink

When you use a LAN uplink, the NMS ignores any profile setting for the port that would override the uplink setting. For example, if you have an iMG1425 using a LAN uplink, you cannot set the LAN interface for Internet, voice or video service.

A LAN uplink uses the management service. You can set the interface as management in the iMG General Profile as a placeholder to ensure the interface is not selected for any other service.

To create a profile to identify a LAN uplink:

1. In the **Network Objects** panel, go to **Network Service Data** > **Profiles**.
2. From the menu, go to **Network Services** > **Profile** > **iMG/RG Service Profiles** > **Create iMG/RG General Profile**. The **Create Profile** box for the RG General profile appears.
3. In the **Profile Name** field, enter a name for the profile.
4. Select the **Port Assignment** tab.
5. Select the port with the LAN uplink. For iMG 1000 and iMG 2000 series devices, select **Port 1**. For AT-624 and AT-634 iMGs, select **Port 4**.
6. In the **Service** drop-down list, select **Management**.



Profile Name:

Profile Type: RG General

Port Assignment: Settings

Port	Service	Speed	Upstream Rate Limit (kbps)	Downstream Rate Limit (kb...	Admin. State
Port 1	None	Autonegotiate	None	None	Disabled
Port 2	None	Autonegotiate	None	None	Disabled
Port 3	None	Autonegotiate	None	None	Disabled
Port 4	None	Autonegotiate	None	None	Disabled
Port 5		Autonegotiate	None	None	Disabled
Port 6		Autonegotiate	None	None	Disabled
Wireless					
HPNA			None	None	Disabled
G-Lan		Autonegotiate	None	None	Disabled

Copy values from profile: GENERAL_MultVC

FIGURE 21-105 iMG General Profile with a LAN Uplink on Port 4

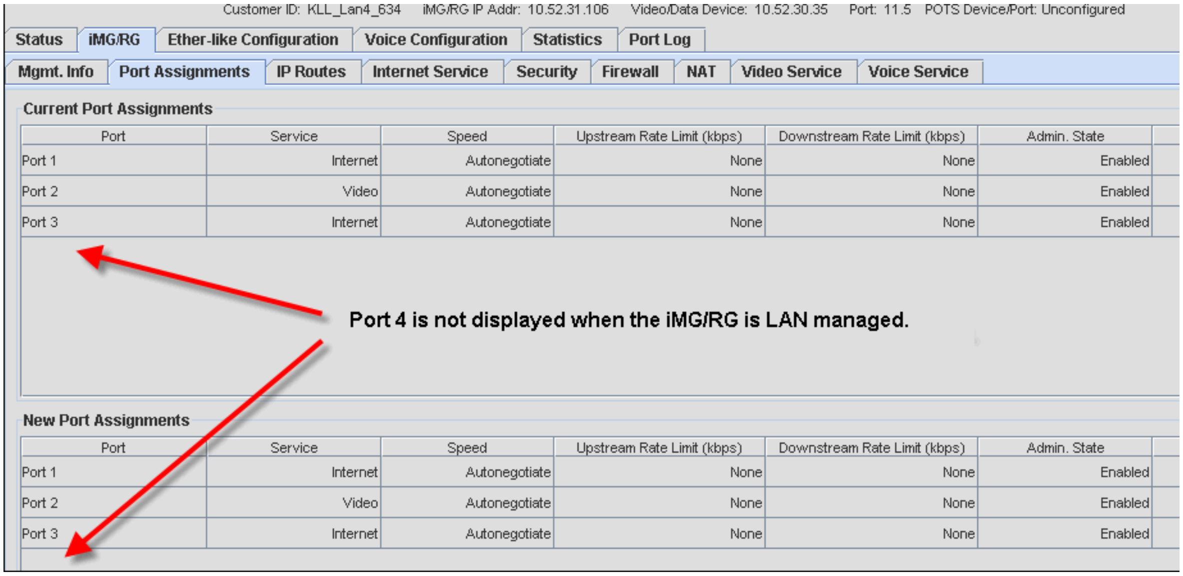
Note: When you select Management for the service, the NMS automatically shows the Admin. State as Enabled.

7. Click **Create** to create the profile.

21.17.4 Service Management with a LAN Uplink

When you view the properties for an iMG with a LAN uplink, the LAN uplink is identified in one of two ways:

- For AT-624 and AT-634 iMGs, the port does not appear in the list of ports on the Port Assignment tab.



Customer ID: KLL_Lan4_634 iMG/RG IP Addr: 10.52.31.106 Video/Data Device: 10.52.30.35 Port: 11.5 POTS Device/Port: Unconfigured

Current Port Assignments

Port	Service	Speed	Upstream Rate Limit (kbps)	Downstream Rate Limit (kbps)	Admin. State
Port 1	Internet	Autonegotiate	None	None	Enabled
Port 2	Video	Autonegotiate	None	None	Enabled
Port 3	Internet	Autonegotiate	None	None	Enabled

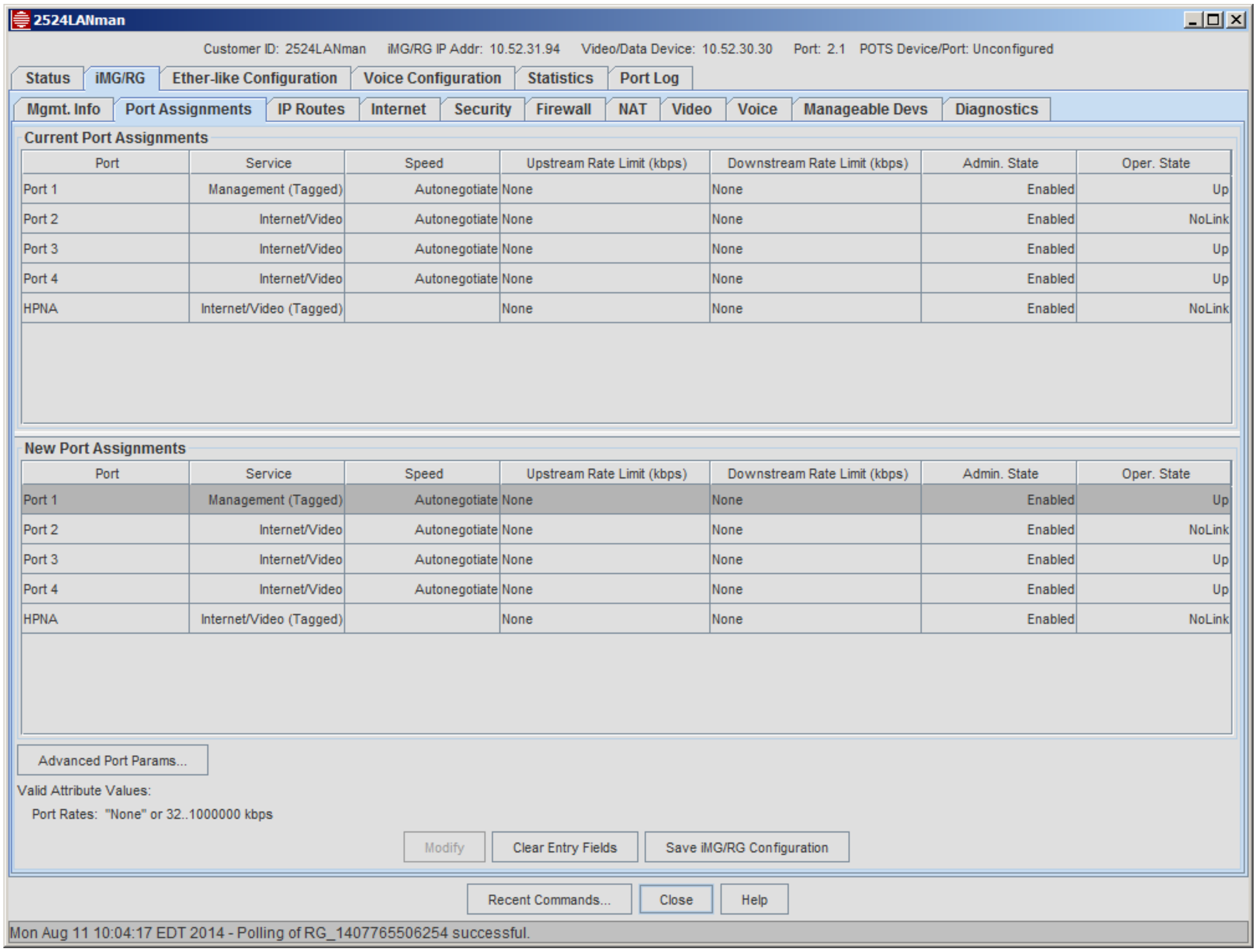
Port 4 is not displayed when the iMG/RG is LAN managed.

New Port Assignments

Port	Service	Speed	Upstream Rate Limit (kbps)	Downstream Rate Limit (kbps)	Admin. State
Port 1	Internet	Autonegotiate	None	None	Enabled
Port 2	Video	Autonegotiate	None	None	Enabled
Port 3	Internet	Autonegotiate	None	None	Enabled

FIGURE 21-106 AT-624 or AT-634 iMG with LAN uplink

- For iMG 1000 or iMG 2000 series iMGs, the port appears with the Management service listed.



Customer ID: 2524LANman iMG/RG IP Addr: 10.52.31.94 Video/Data Device: 10.52.30.30 Port: 2.1 POTS Device/Port: Unconfigured

Current Port Assignments

Port	Service	Speed	Upstream Rate Limit (kbps)	Downstream Rate Limit (kbps)	Admin. State	Oper. State
Port 1	Management (Tagged)	Autonegotiate	None	None	Enabled	Up
Port 2	Internet/Video	Autonegotiate	None	None	Enabled	NoLink
Port 3	Internet/Video	Autonegotiate	None	None	Enabled	Up
Port 4	Internet/Video	Autonegotiate	None	None	Enabled	Up
HPNA	Internet/Video (Tagged)		None	None	Enabled	NoLink

New Port Assignments

Port	Service	Speed	Upstream Rate Limit (kbps)	Downstream Rate Limit (kbps)	Admin. State	Oper. State
Port 1	Management (Tagged)	Autonegotiate	None	None	Enabled	Up
Port 2	Internet/Video	Autonegotiate	None	None	Enabled	NoLink
Port 3	Internet/Video	Autonegotiate	None	None	Enabled	Up
Port 4	Internet/Video	Autonegotiate	None	None	Enabled	Up
HPNA	Internet/Video (Tagged)		None	None	Enabled	NoLink

Valid Attribute Values:

Port Rates: "None" or 32..1000000 kbps

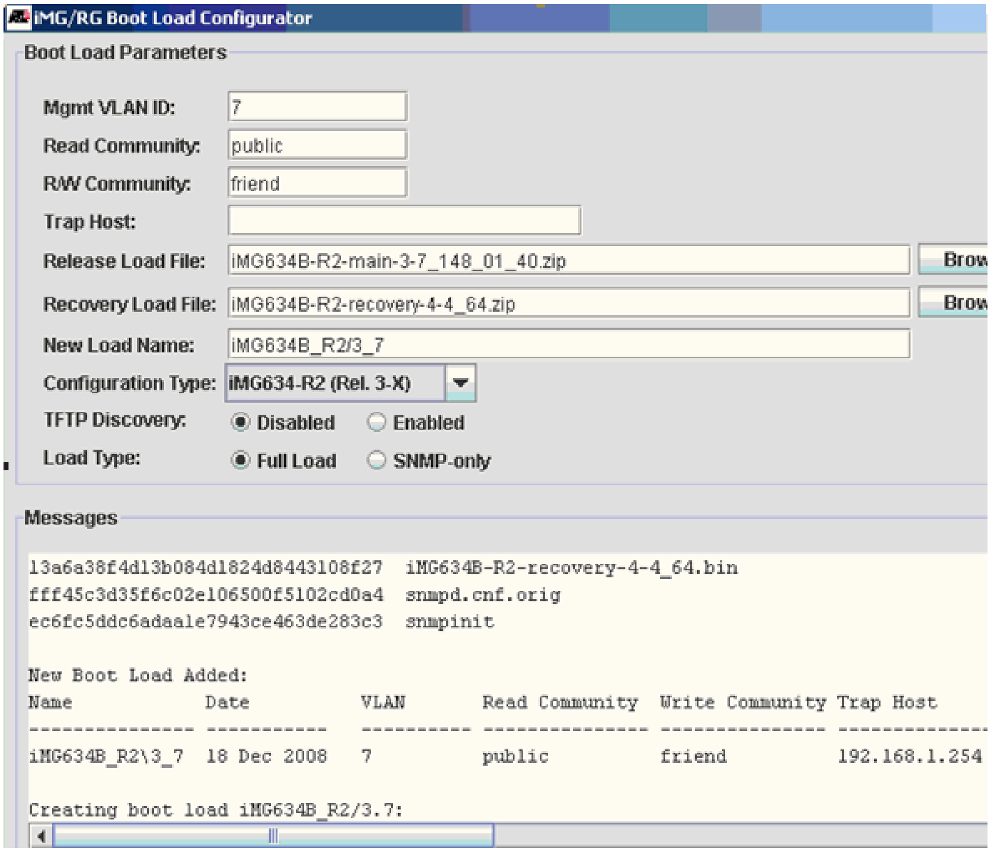
Mon Aug 11 10:04:17 EDT 2014 - Polling of RG_1407765506254 successful.

FIGURE 21-107 iMG 1000 or iMG 2000 series iMG with LAN uplink

21.17.5 Example: Installing an AT-624 or AT-634 Series iMG with a LAN Uplink

In this example, an AT-iMG634B-R2 iMG is pre-provisioned with the NMS. The customer connects the LAN4 port as the uplink and powers up the iMG.

1. Ensure the correct firmware and bootstrap files available and are loaded using the iMG Boot Load Configurator. The following figure is an example of how the configurator should be data filled.



Boot Load Parameters

Mgmt VLAN ID:	7
Read Community:	public
R/W Community:	friend
Trap Host:	
Release Load File:	iMG634B-R2-main-3-7_148_01_40.zip
Recovery Load File:	iMG634B-R2-recovery-4-4_64.zip
New Load Name:	iMG634B_R2/3_7
Configuration Type:	iMG634-R2 (Rel. 3-X)
TFTP Discovery:	● Disabled ○ Enabled
Load Type:	● Full Load ○ SNMP-only

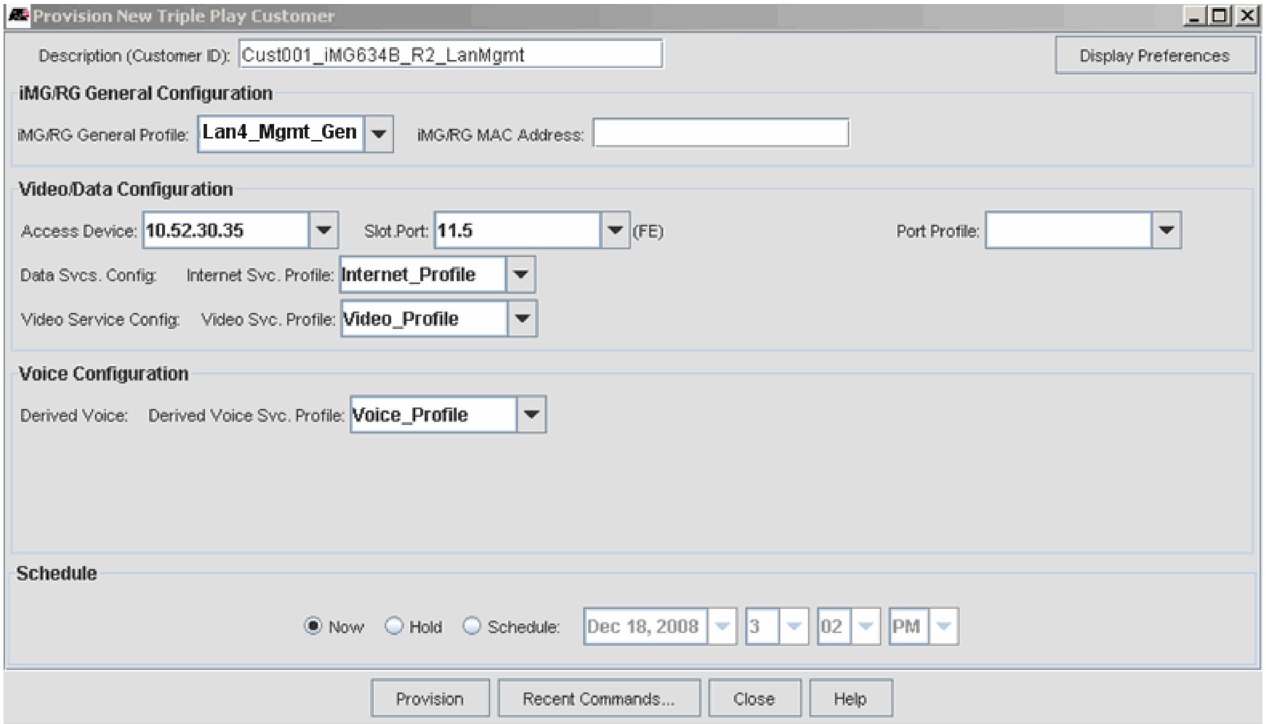
Messages

```
13a6a38f4d13b084d1824d8443108f27  iMG634B-R2-recovery-4-4_64.bin
fff45c3d35f6c02e106500f5102cd0a4  snmpd.cnf.orig
ec6fc5ddc6adaale7943ce463de283c3  snmpinit

New Boot Load Added:
Name            Date         VLAN       Read Community  Write Community Trap Host
--------------- -----------  ---------- --------------- --------------- --------------
iMG634B_R2\3_7  18 Dec 2008  7          public          friend          192.168.1.254

Creating boot load iMG634B_R2/3.7:
```

FIGURE 21-108 Boot Configurator for 3-7 Device

2. If not already created, create the relevant profiles that are needed. The only difference between these profiles and the ones for an ADSL uplink is the Port Assignment tab, as shown in Figure 21-106.

3. Use the Triple-Play form and provision the customer, using the profiles created in Step 2. The uplink port is an FE. Refer to the following figure.



Description (Customer ID): Cust001_iMG634B_R2_LanMgmt

iMG/RG General Configuration

iMG/RG General Profile: Lan4_Mgmt_Gen iMG/RG MAC Address:

Video/Data Configuration

Access Device: 10.52.30.35 Slot.Port: 11.5 (FE) Port Profile:

Data Svcs. Config: Internet Svc. Profile: Internet_Profile

Video Service Config: Video Svc. Profile: Video_Profile

Voice Configuration

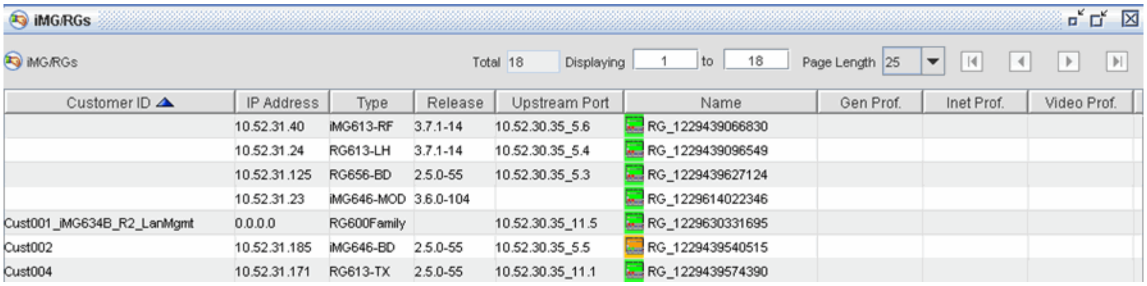
Derived Voice: Derived Voice Svc. Profile: Voice_Profile

Schedule

● Now ○ Hold ○ Schedule: Dec 18, 2008 3 02 PM

FIGURE 21-109 Triple-Play form Using General Profile for LAN4

4. Review the iMG/RG table. Note that there are still no associated profiles and no IP address, as shown in the following figure.

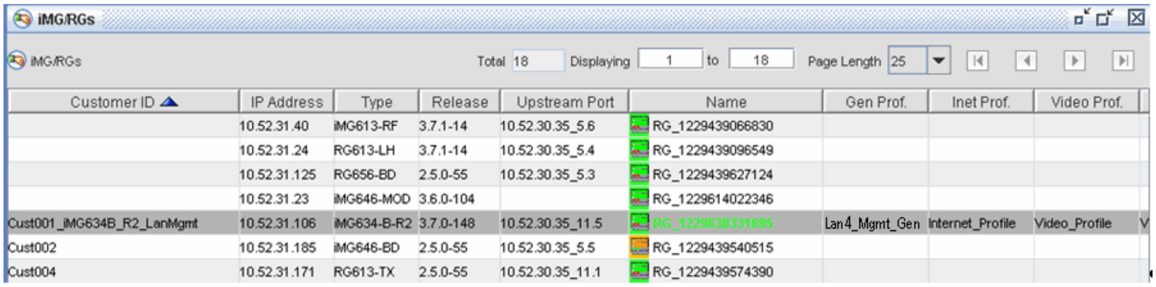


Total 18 Displaying 1 to 18 Page Length 25

Customer ID	IP Address	Type	Release	Upstream Port	Name	Gen Prof.	Inet Prof.	Video Prof.
	10.52.31.40	iMG613-RF	3.7.1-14	10.52.30.35_5.6	RG_1229439066830			
	10.52.31.24	RG613-LH	3.7.1-14	10.52.30.35_5.4	RG_1229439096549			
	10.52.31.125	RG656-BD	2.5.0-55	10.52.30.35_5.3	RG_1229439627124			
	10.52.31.23	iMG646-MOD	3.6.0-104		RG_1229614022346			
Cust001_iMG634B_R2_LanMgmt	0.0.0.0	RG600Family		10.52.30.35_11.5	RG_1229630331695			
Cust002	10.52.31.185	iMG646-BD	2.5.0-55	10.52.30.35_5.5	RG_1229439540515			
Cust004	10.52.31.171	RG613-TX	2.5.0-55	10.52.30.35_11.1	RG_1229439574390			

FIGURE 21-110 iMG Pre-provisioned

5. Connect the customer equipment to one or more LAN ports 1, 2, and 3.
6. Plug the ethernet uplink into LAN4.
7. Power on the iMG.
8. Wait and observe how the iMG is discovered, an IP address is found, and the profiles are applied. Refer to the following figure.



Customer ID ▲	IP Address	Type	Release	Upstream Port	Name	Gen Prof.	Inet Prof.	Video Prof.	
	10.52.31.40	iMG613-RF	3.7.1-14	10.52.30.35_5.6	RG_1229439066830				
	10.52.31.24	RG613-LH	3.7.1-14	10.52.30.35_5.4	RG_1229439096549				
	10.52.31.125	RG656-BD	2.5.0-55	10.52.30.35_5.3	RG_1229439627124				
	10.52.31.23	iMG646-MOD	3.6.0-104		RG_1229614022346				
Cust001_iMG634B_R2_LanMgmt	10.52.31.106	iMG634-B-R2	3.7.0-148	10.52.30.35_11.5	RG_1229638331695	Lan4_Mgmt_Gen	Internet_Profile	Video_Profile	V
Cust002	10.52.31.185	iMG646-BD	2.5.0-55	10.52.30.35_5.5	RG_1229439540515				
Cust004	10.52.31.171	RG613-TX	2.5.0-55	10.52.30.35_11.1	RG_1229439574390				

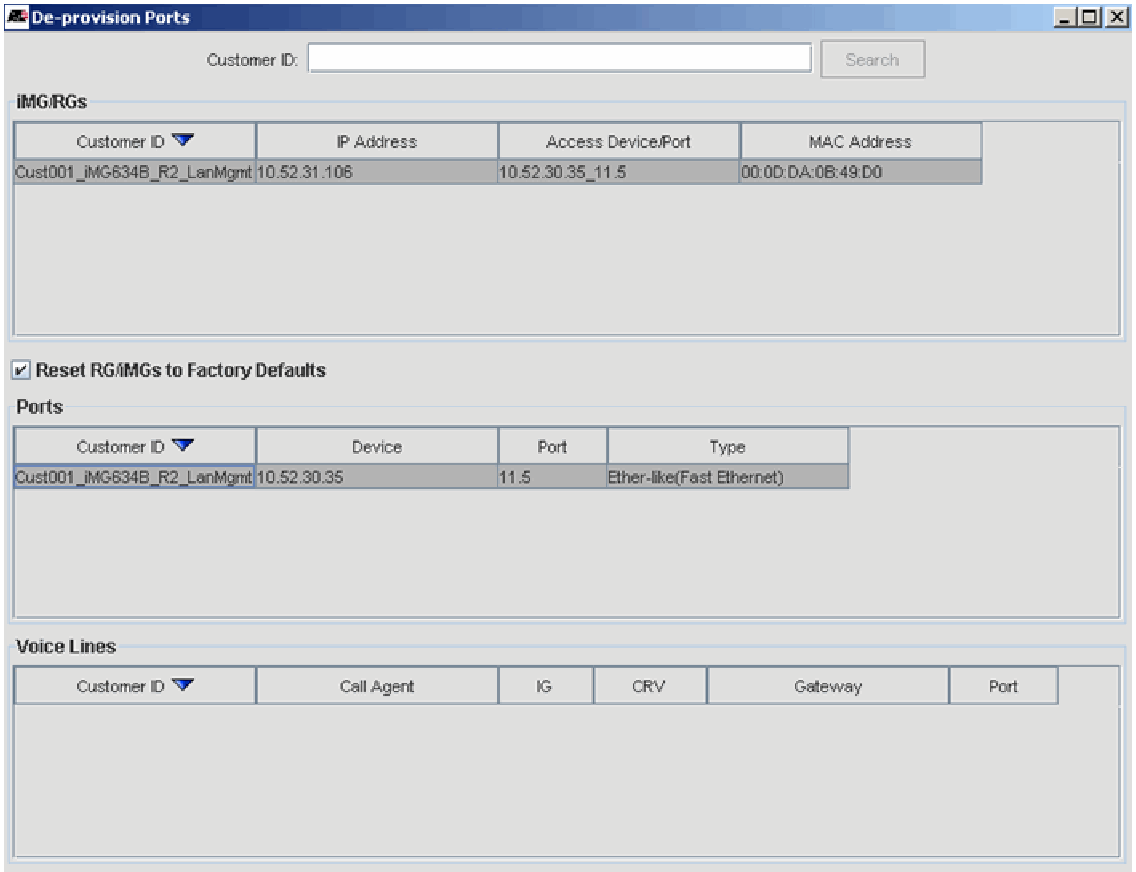
FIGURE 21-111 iMG Provisioned using LAN4

9. The tabs for the Details screen are the same as an ADSL uplink, with the one difference the Port Assignments tab has no port 4, as shown in Figure 21-106.

21.17.6 Example: Deprovisioning an AT-624 or AT-634 Series iMG and Reprovisioning with the ADSL Uplink

In this example, an iMG that currently uses LAN4 for the uplink is deprovisioned and then reprovisioned using the ADSL port as the uplink.

1. Right click on the iMG and select **De-provision Customer iMG/RG**. Select all of the options, as shown in the following figure.



Customer ID ▼	IP Address	Access Device/Port	MAC Address
Cust001_iMG634B_R2_LanMgmt	10.52.31.106	10.52.30.35_11.5	00:0D:DA:0B:49:D0

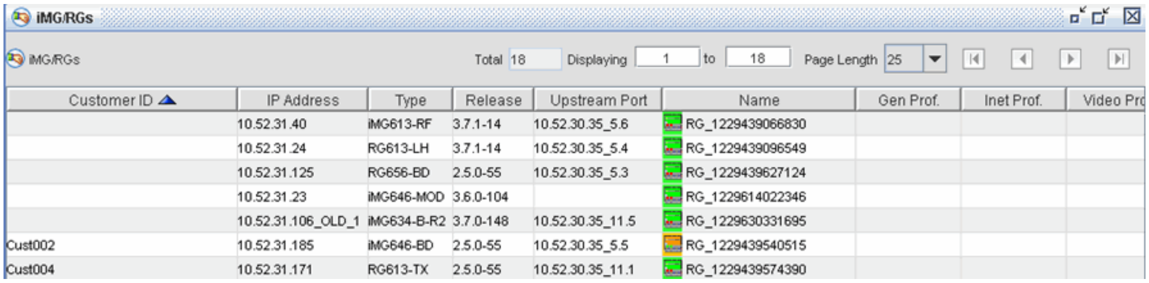
☑ Reset RG/iMGs to Factory Defaults

Customer ID ▼	Device	Port	Type
Cust001_iMG634B_R2_LanMgmt	10.52.30.35	11.5	Ether-like(Fast Ethernet)

Customer ID ▼	Call Agent	IG	CRV	Gateway	Port

FIGURE 21-112 Deprovision iMG - Reset to Factory Defaults

2. Note in the iMG/RG list that the device has all of the profiles dropped and the IP address is appended with _OLD, since the IP address is now released. Refer to the following figure.



iMG/RGs

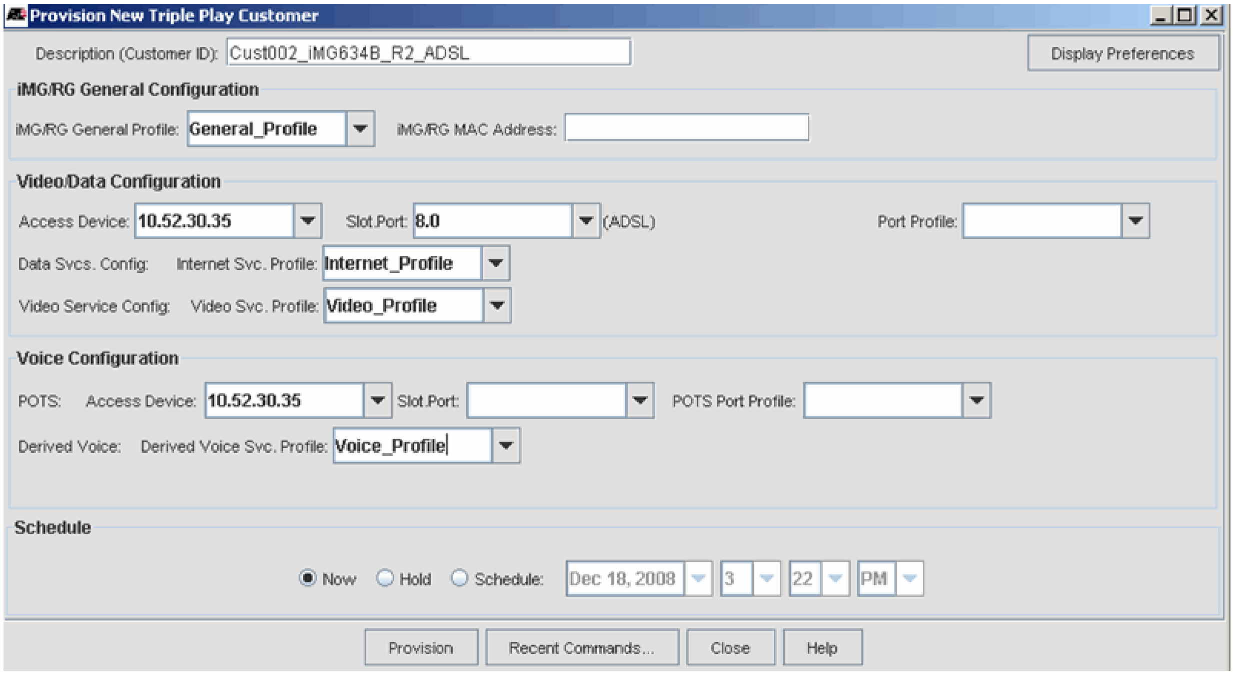
iMG/RGs Total 18 Displaying 1 to 18 Page Length 25

Customer ID ▲	IP Address	Type	Release	Upstream Port	Name	Gen Prof.	Inet Prof.	Video Pro
	10.52.31.40	iMG613-RF	3.7.1-14	10.52.30.35_5.6	🟩 RG_1229439066830			
	10.52.31.24	RG613-LH	3.7.1-14	10.52.30.35_5.4	🟩 RG_1229439096549			
	10.52.31.125	RG656-BD	2.5.0-55	10.52.30.35_5.3	🟩 RG_1229439627124			
	10.52.31.23	iMG646-MOD	3.6.0-104		🟩 RG_1229614022346			
	10.52.31.106_OLD_1	iMG634-B-R2	3.7.0-148	10.52.30.35_11.5	🟩 RG_1229630331695			
Cust002	10.52.31.185	iMG646-BD	2.5.0-55	10.52.30.35_5.5	🟧 RG_1229439540515			
Cust004	10.52.31.171	RG613-TX	2.5.0-55	10.52.30.35_11.1	🟩 RG_1229439574390			

FIGURE 21-113 iMG De provisioned

3. If not done already, create profiles for the iMG. If the service/VLAN configuration is the same, the only profile that is different is the General Profile, with the Port Assignments tab having port 4 not set to Management.

4. Fill in the Triple Play Form with the profiles, and select an ADSL port for the Slot.Port, as shown in the following figure.



Provision New Triple Play Customer

Description (Customer ID): Cust002_iMG634B_R2_ADSL

iMG/RG General Configuration

iMG/RG General Profile: General_Profile

iMG/RG MAC Address:

Video/Data Configuration

Access Device: 10.52.30.35 Slot.Port: 8.0 (ADSL) Port Profile:

Data Svcs. Config: Internet Svc. Profile: Internet_Profile

Video Service Config: Video Svc. Profile: Video_Profile

Voice Configuration

POTS: Access Device: 10.52.30.35 Slot.Port: POTS Port Profile:

Derived Voice: Derived Voice Svc. Profile: Voice_Profile

Schedule

● Now ○ Hold ○ Schedule: Dec 18, 2008 3 22 PM

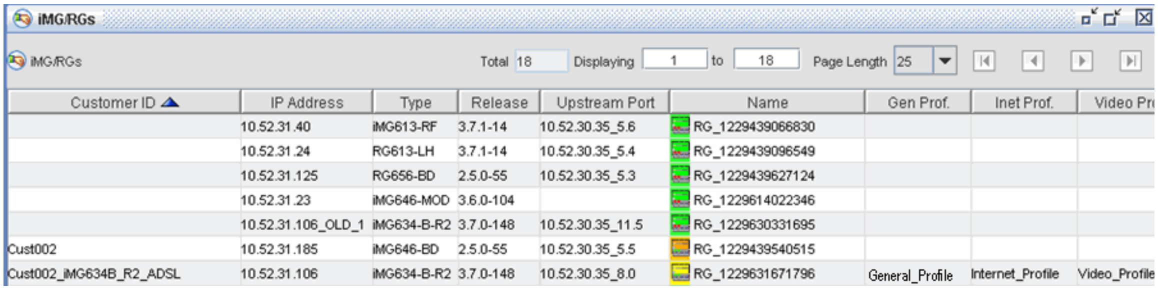
FIGURE 21-114 Triple Play for ADSL Mgmt

5. Connect the customer equipment to one or more LAN ports 1, 2, 3, and 4.

6. Plug the uplink ADSL into the ADSL port.

7. Power on the iMG.

8. Wait and observe how the iMG is discovered, an IP address is found, and the profiles are applied. Refer to the following figure.



Total 18 Displaying 1 to 18 Page Length 25

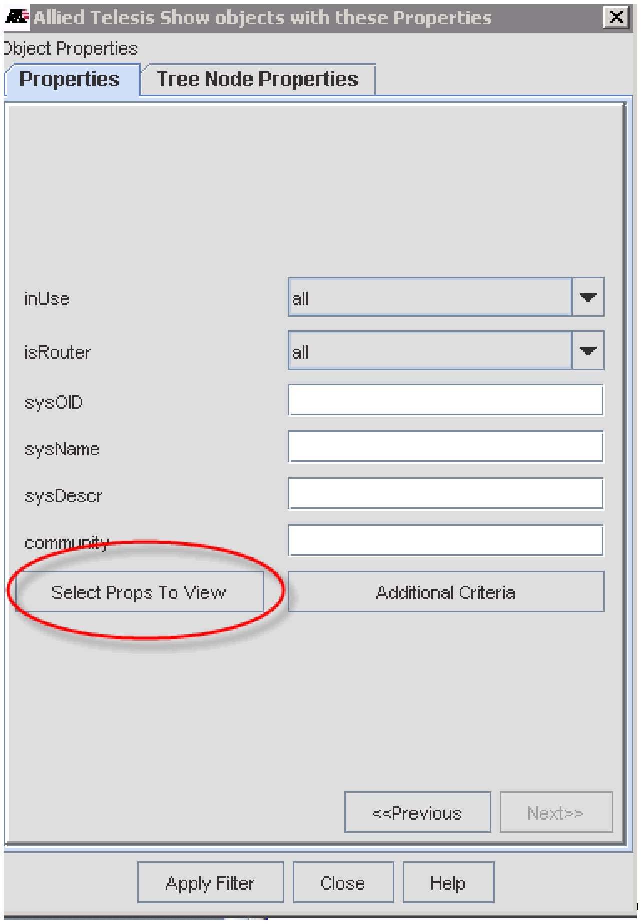
Customer ID	IP Address	Type	Release	Upstream Port	Name	Gen Prof.	Inet Prof.	Video Pr
	10.52.31.40	iMG613-RF	3.7.1-14	10.52.30.35_5.6	RG_1229439066830			
	10.52.31.24	RG613-LH	3.7.1-14	10.52.30.35_5.4	RG_1229439096549			
	10.52.31.125	RG656-BD	2.5.0-55	10.52.30.35_5.3	RG_1229439627124			
	10.52.31.23	iMG646-MOD	3.6.0-104		RG_1229614022346			
	10.52.31.106_OLD_1	iMG634-B-R2	3.7.0-148	10.52.30.35_11.5	RG_1229630331695			
Cust002	10.52.31.185	iMG646-BD	2.5.0-55	10.52.30.35_5.5	RG_1229439540515			
Cust002_iMG634B_R2_ADSL	10.52.31.106	iMG634-B-R2	3.7.0-148	10.52.30.35_8.0	RG_1229631671796	General_Profile	Internet_Profile	Video_Profile

FIGURE 21-115 iMG Provisioned using ADSL (no longer LAN4)

9. Note that in the Customer Details form, the Port Assignments tab now has port 4.

21.17.7 Creating Custom Views for AT-624 and AT-634 iMGs with a LAN Uplink

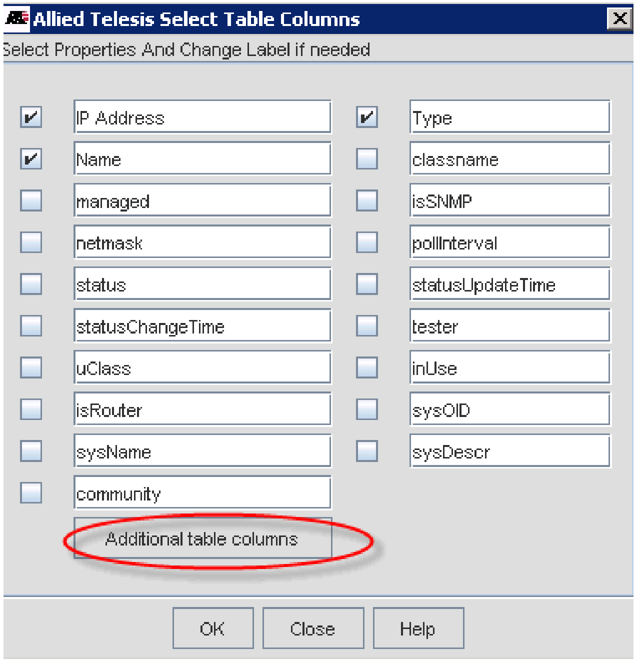
You can set up a custom view to show which iMG is running on ADSL vs. LAN 4. This is done by right clicking on the iMG/RGs entry in the Network Inventory, and selecting *Custom Views -> Add Custom View*. In the Custom View wizard under the “Properties” tab, choose the “Select Props To View” button, as shown in the following figure.



inUse: all
isRouter: all
sysOID:
sysName:
sysDescr:
community:

FIGURE 21-116 Selecting Properties for a Custom View

In the next frame that opens select the “Additional table Columns” button, as shown in the following figure.



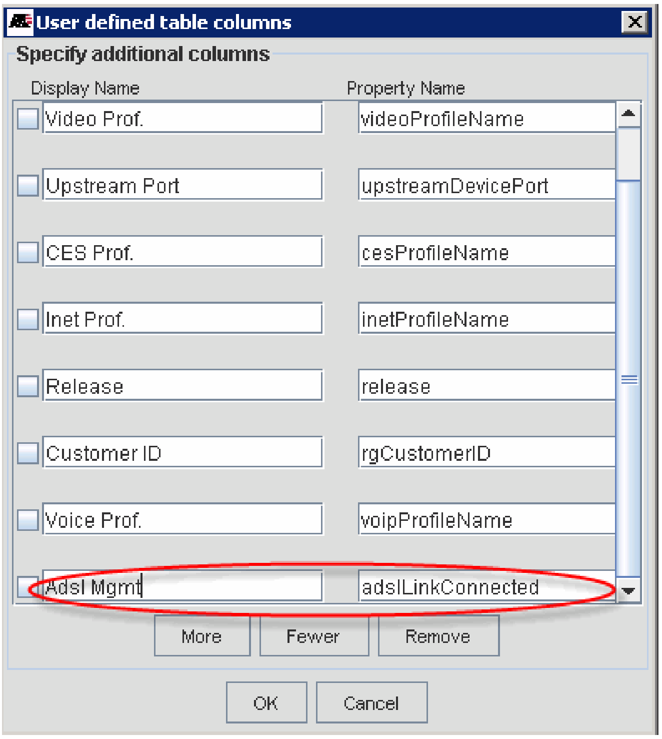
Allied Telesis Select Table Columns

Select Properties And Change Label if needed

☑	IP Address	☑	Type
☑	Name	☐	classname
☐	managed	☐	isSNMP
☐	netmask	☐	pollInterval
☐	status	☐	statusUpdateTime
☐	statusChangeTime	☐	tester
☐	uClass	☐	inUse
☐	isRouter	☐	sysOID
☐	sysName	☐	sysDescr
☐	community		

FIGURE 21-117 Selecting Additional Table Columns

From here additional properties that are in the database can be entered and labeled. In our case the property we need to enter is “adslLinkConnected”, the label chosen for this example is “Adsl Mgmt”, indicating whether the iMG/RG is managed via an ADSL port. Refer to the following figure.



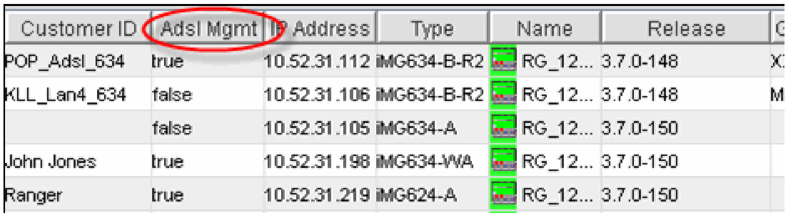
User defined table columns

Specify additional columns

	Display Name	Property Name
☐	Video Prof.	videoProfileName
☐	Upstream Port	upstreamDevicePort
☐	CES Prof.	cesProfileName
☐	Inet Prof.	inetProfileName
☐	Release	release
☐	Customer ID	rgCustomerID
☐	Voice Prof.	voipProfileName
☐	Adsl Mgmt	adslLinkConnected

FIGURE 21-118 Adding AdslMgmt Column

The end result of apply this custom view is shown below. The top two RGs show an ADSL managed 634B-R2 box and a LAN4 managed 634B-R2 device, as shown in the following figure.

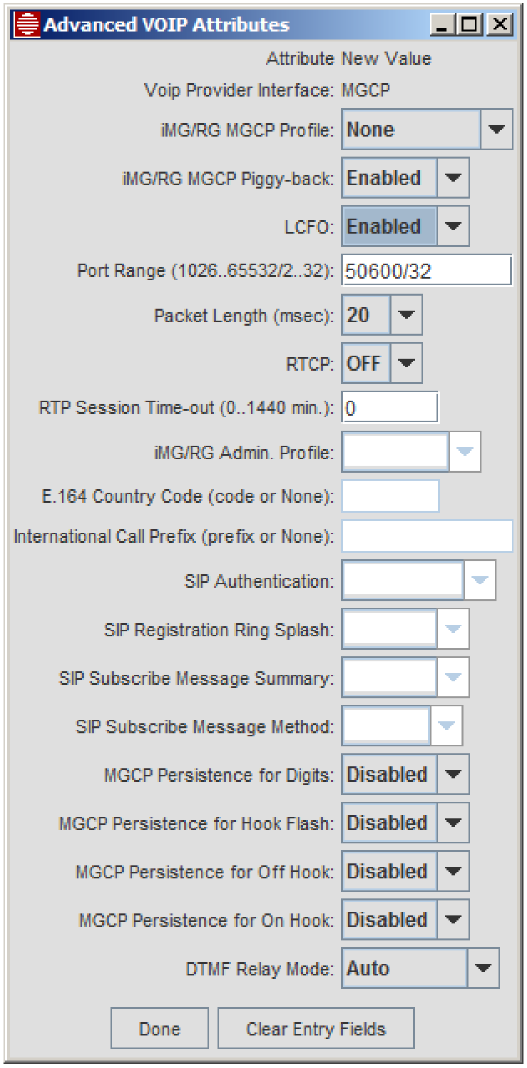


Customer ID	Adsl Mgmt	IP Address	Type	Name	Release	G
POP_Adsl_634	true	10.52.31.112	iMG634-B-R2	RG_12...	3.7.0-148	X
KLL_Lan4_634	false	10.52.31.106	iMG634-B-R2	RG_12...	3.7.0-148	M
	false	10.52.31.105	iMG634-A	RG_12...	3.7.0-150	
John Jones	true	10.52.31.198	iMG634-WA	RG_12...	3.7.0-150	
Ranger	true	10.52.31.219	iMG624-A	RG_12...	3.7.0-150	

FIGURE 21-119 ADSL Mgmt Column as False if has LAN4 Mgmt

21.18 Advanced VOIP Attributes

The Advanced VOIP Attributes box contains VOIP parameters for iMGs. The active fields vary depending on whether the VOIP type is MGCP or SIP.



Advanced VOIP Attributes

Attribute New Value

Voip Provider Interface: MGCP

iMG/RG MGCP Profile: None

iMG/RG MGCP Piggy-back: Enabled

LCFO: Enabled

Port Range (1026..65532/2..32): 50600/32

Packet Length (msec): 20

RTCP: OFF

RTP Session Time-out (0..1440 min.): 0

iMG/RG Admin. Profile:

E.164 Country Code (code or None):

International Call Prefix (prefix or None):

SIP Authentication:

SIP Registration Ring Splash:

SIP Subscribe Message Summary:

SIP Subscribe Message Method:

MGCP Persistence for Digits: Disabled

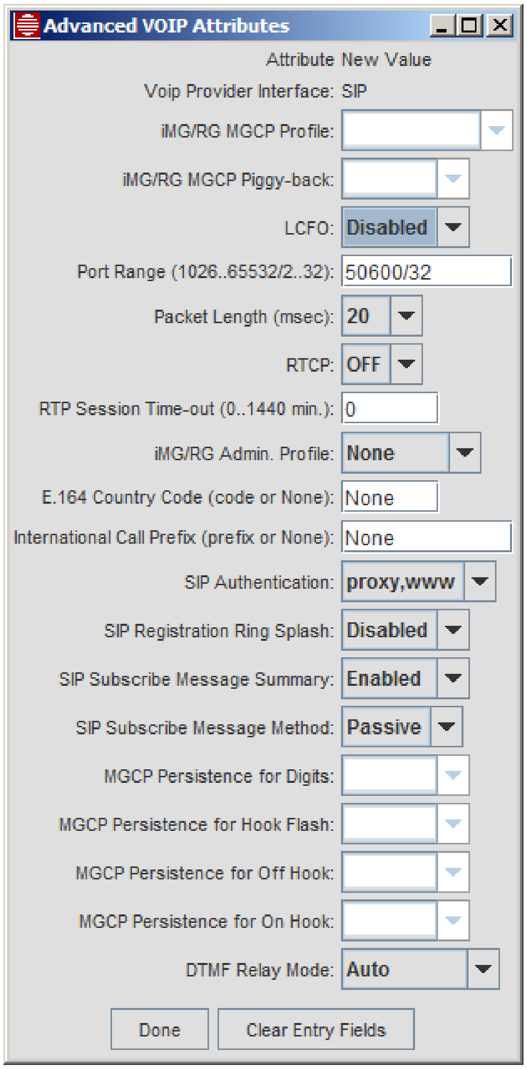
MGCP Persistence for Hook Flash: Disabled

MGCP Persistence for Off Hook: Disabled

MGCP Persistence for On Hook: Disabled

DTMF Relay Mode: Auto

FIGURE 21-120 Advanced VOIP Attributes (MGCP)



Attribute	New Value
Voip Provider Interface:	SIP
iMG/RG MGCP Profile:	
iMG/RG MGCP Piggy-back:	
LCFO:	Disabled
Port Range (1026..65532/2..32):	50600/32
Packet Length (msec):	20
RTCP:	OFF
RTP Session Time-out (0..1440 min.):	0
iMG/RG Admin. Profile:	None
E.164 Country Code (code or None):	None
International Call Prefix (prefix or None):	None
SIP Authentication:	proxy,www
SIP Registration Ring Splash:	Disabled
SIP Subscribe Message Summary:	Enabled
SIP Subscribe Message Method:	Passive
MGCP Persistence for Digits:	
MGCP Persistence for Hook Flash:	
MGCP Persistence for Off Hook:	
MGCP Persistence for On Hook:	
DTMF Relay Mode:	Auto

FIGURE 21-121 Advanced VOIP Attributes (SIP)

21.18.1 LCFO

The Loop Current Feed Open option is used to indicate that the calling/called party has gone onhook and is a useful feature for businesses that have key systems that transfer calls. This is available on all iMGs that are 3-7 and up. Both MGCP and SIP are supported.

The LCFO option is displayed from the **Advanced VOIP Params** button that is on both the Port Management View/Modify “Voice Service” tab, and the iMG/RG Voice Service Profile display. When LCFO is enabled, it applies to all VoIP lines on the iMG/RG.

21.18.2 SIP Subscribe Message Summary

SIP Subscribe Message Summary controls how an iMG receives notifications for events such as Message-Waiting Indication (MWI) from the SIP call server. Depending on the SIP call server, the SIP Subscribe Message Method may or may not be required for receiving the notifications. You can configure iMG devices to receive notifcations either with or without the SUBSCRIBE method.

For iMG devices running software release 4.2.2 and earlier, the options for **SIP Subscribe Message Summary** are:

- **Disabled** - Applies to call servers that do not require SIP Subscribe. Notifications are enabled.
- **Enabled** - Applies to call servers that require SIP Subscribe. Notifications are enabled.

For iMGs running software release 4.2.3 and later, the options for **SIP Subscribe Message Summary** are:

- **Disabled** - Support for notifications is disabled on the iMG.
- **Enabled/Passive** - Applies to call servers that do not require SIP Subscribe. Notifications are enabled.
- **Enabled/Active** - Applies to call servers that require SIP Subscribe. Notifications are enabled.

21.18.3 MGCP Persistence

For iMG 1000 and iMG 2000 devices running software release 4.3 and later, you can configure four parameters for MGCP Persistence: Digits, Hook Flash, Off Hook and On Hook. The following rules apply:

- The parameters apply to MGCP profiles only, such as Genband C15 and Metaswitch. They are grayed out when the VOIP type is SIP.
- For MGCP NCS profiles, such as a Genband profile for the G6, the MGCP Persistence settings for Hook Flash, On Hook and Off Hook are always enabled and changes to these settings are ignored. MGCP Persistence for Digits is disabled by default but you can change it to enabled if necessary.

21.19 iMG/RG Diagnostics

This section lists and describes the diagnostic features that are available for the various iMG/RG models.

21.19.1 iMG GR-909 Diagnostics

The NMS supports GR-909 diagnostics for the following voice-enabled devices:

- MOD iMGs and the iMG726-BD-ON running software release 3.7.4 or higher
- iMGs running software release 4.3 or higher *except* models iMG1525 and iMG1525RF. These two models do not support GR-909 diagnostics.

GR-909 diagnostics includes internal and external tests. For internal tests, the physical wiring is disconnected from the device for the test so only the internal circuitry is tested. For external tests the wiring remains intact and the whole system is tested.

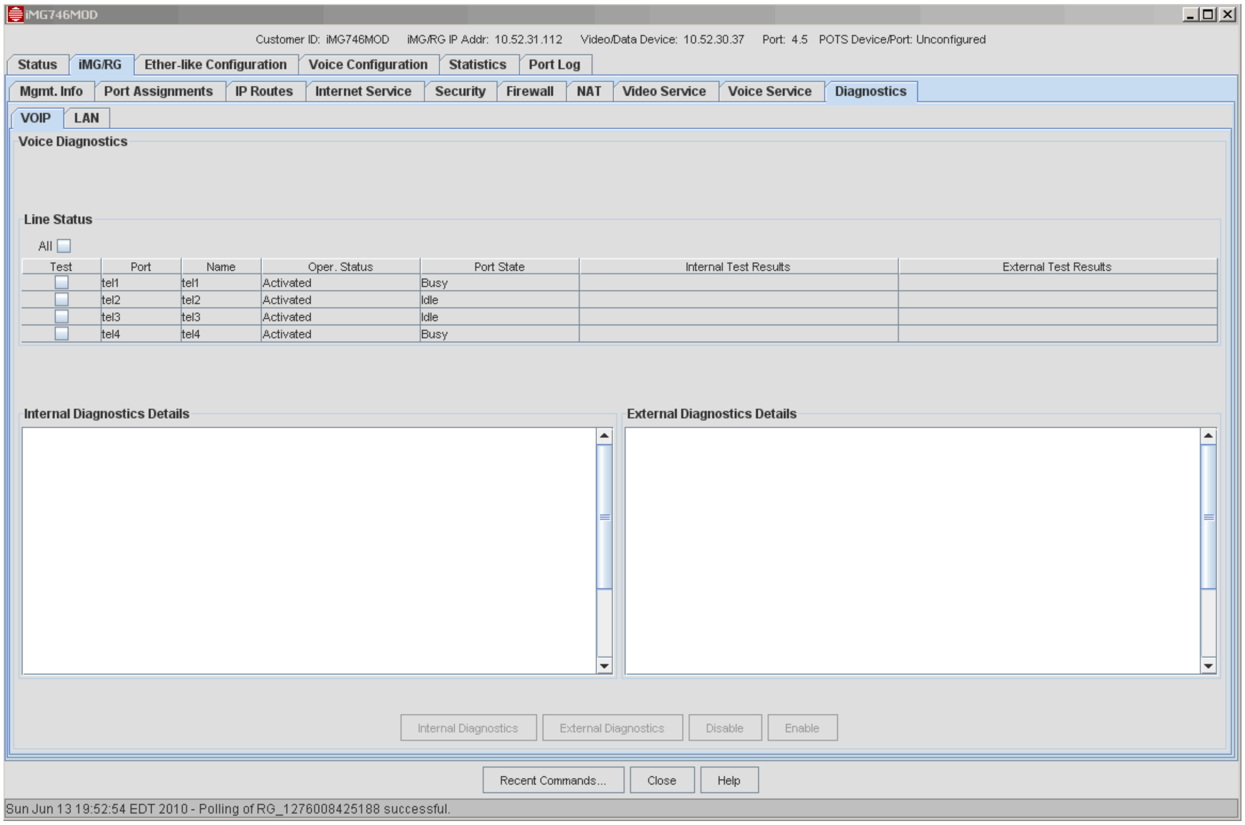
For MOD iMGs and the iMG726-BD-ON, you can display GR-909 internal and external tests as well as voice line status and diagnostic results. You can also disable and enable voice lines from the panel. iMGs running software release 4.3 or higher display external GR-909 diagnostics only.

To run GR-909 diagnostics on an iMG:

1. In the **Network Objects** panel, select **Network Inventory > iMG/RGs** to open the **iMG/RGs** screen.
2. Select the desired iMG, right-click and select **View/Modify Details**.
3. Select the **iMG/RG** tab, then select the **Diagnostics** tab.
4. In the **Diagnostics** panel, select the **VOIP** tab to display the **Voice Diagnostics** panel.

Note: For MOD iMGs and the iMG726-BD-ON, the Diagnostics panel contains two tabs: VOIP and LAN. For iMGs running software release 4.3 or higher, the Diagnostics panel contains just the VOIP tab.

The **Voice Diagnostics** panel display varies depending on the iMG.

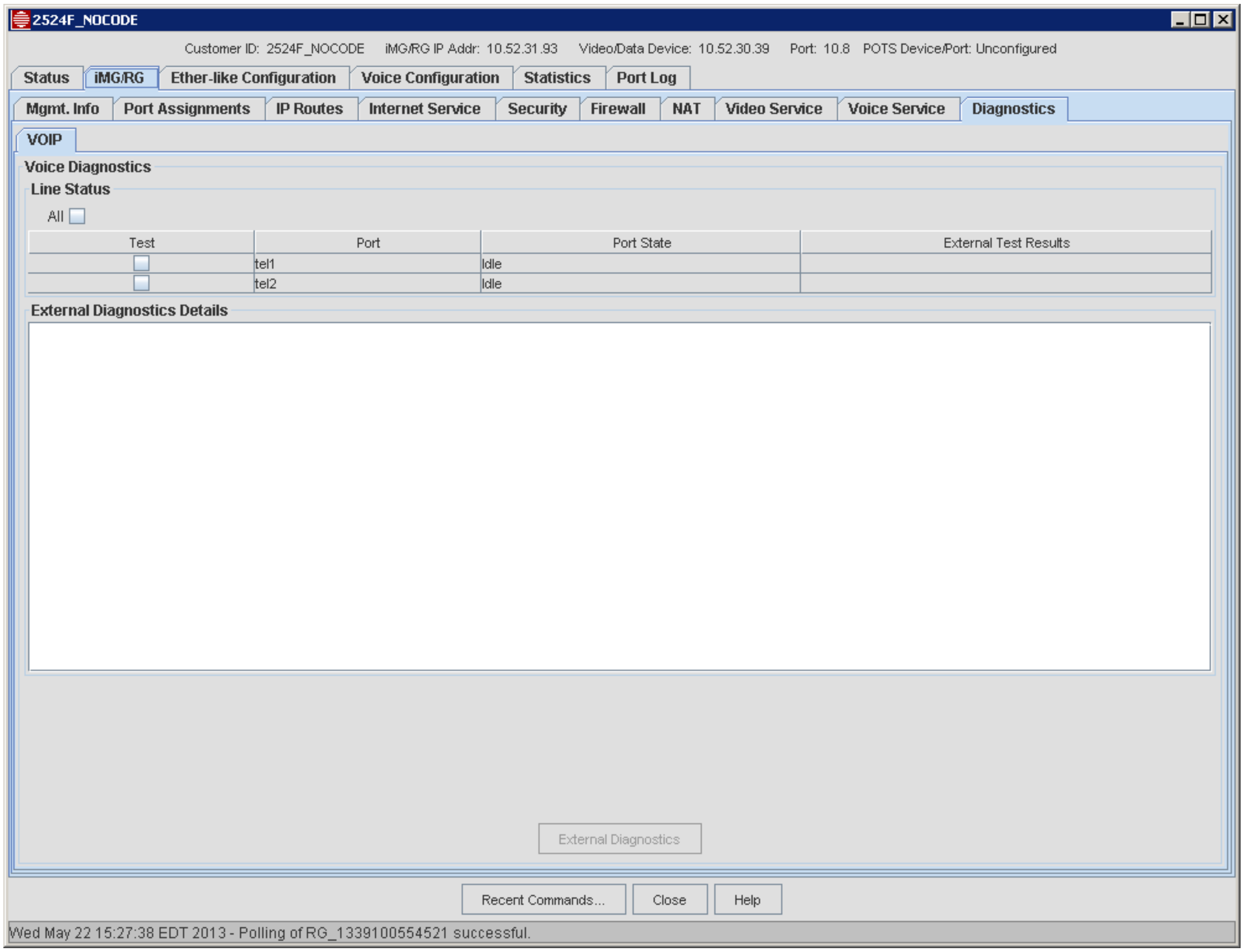


Customer ID: iMG746MOD iMG/RG IP Addr: 10.52.31.112 Video/Data Device: 10.52.30.37 Port: 4.5 POTS Device/Port: Unconfigured

Test	Port	Name	Oper. Status	Port State	Internal Test Results	External Test Results
☐	tel1	tel1	Activated	Busy		
☐	tel2	tel2	Activated	Idle		
☐	tel3	tel3	Activated	Idle		
☐	tel4	tel4	Activated	Busy		

Sun Jun 13 19:52:54 EDT 2010 - Polling of RG_1276008425188 successful.

FIGURE 21-122 Voice Diagnostics panel for MOD iMGs and iMG726-BD-ON



Customer ID: 2524F_NOCODE iMG/RG IP Addr: 10.52.31.93 Video/Data Device: 10.52.30.39 Port: 10.8 POTS Device/Port: Unconfigured

All □

Test	Port	Port State	External Test Results
□	tel1	Idle	
□	tel2	Idle	

Wed May 22 15:27:38 EDT 2013 - Polling of RG_1339100554521 successful.

FIGURE 21-123 Voice Diagnostics panel for R4.3 and higher iMGs

The Line Status table displays each enabled voice port on the iMG and its current status.

TABLE 21-14

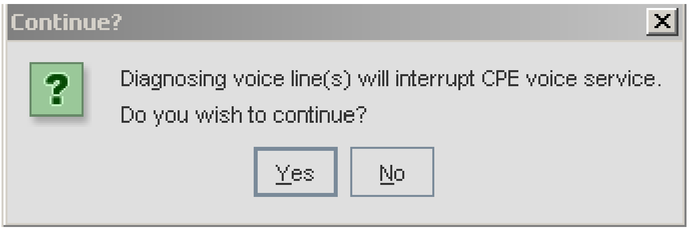
MOD iMG and iMG726-BD-ON	R4.3 and higher iMGs
Port	Port
Name	Port State
Operational Status	
Port State	

These are polled from the device and updated approximately every 30 seconds while the panel is active.

5. To select a row, check the box in the **Test** column. Check the **All** box to select all of the rows at once.

Caution: Testing all of the interfaces at once will increase the duration of the test and interrupt CPE voice service.

A confirmation box appears.



Diagnosing voice line(s) will interrupt CPE voice service.
Do you wish to continue?

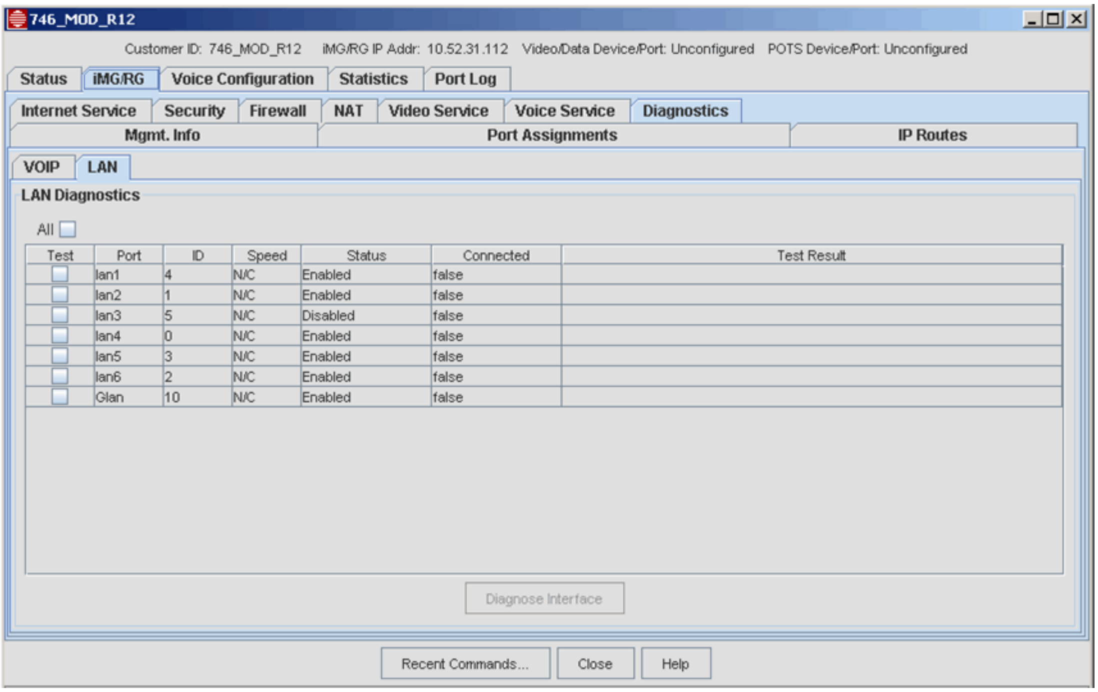
FIGURE 21-124 Warning when Diagnosing VOIP Lines

6. Click **Yes** to run the test. The results of the test are displayed in the Test Results fields in the table and the last diagnostic results are displayed in the Diagnostic Details panels.

21.19.2 iMG LAN Diagnostics

MOD iMGs and the iMG726-BD-ON running software release 3.7.4 or higher support LAN diagnostics. With the NMS, you can diagnose CPE LAN ports. This diagnosis will detect faults in the subscriber's private network cables. The GUI allows you to select any or all CPE switch ports, diagnose them, and see the results.

The LAN Diagnostics Panel is added to the Triple-Play Service Management form for the iMG. The LAN Diagnostics belongs to the iMG/RG Diagnostics sub-tab, but it is only displayed if the iMG/RG is an iMG726-BD-ON, iMG6x6MOD or iMG7x6MOD CPE. Refer to the following figure.



Customer ID: 746_MOD_R12 iMG/RG IP Addr: 10.52.31.112 Video/Data Device/Port: Unconfigured POTS Device/Port: Unconfigured

LAN Diagnostics

All ☐

Test	Port	ID	Speed	Status	Connected	Test Result
☐	lan1	4	N/C	Enabled	false	
☐	lan2	1	N/C	Enabled	false	
☐	lan3	5	N/C	Disabled	false	
☐	lan4	0	N/C	Enabled	false	
☐	lan5	3	N/C	Enabled	false	
☐	lan6	2	N/C	Enabled	false	
☐	Glan	10	N/C	Enabled	false	

FIGURE 21-125 LAN Diagnostics Tab for iMG726-BD-ON and MOD-type iMG

Initially the table displays each LAN port on the iMG and its current status.

Not all modules include a Glan interface; if the Glan interface is not present, the Glan row will be omitted from the table.

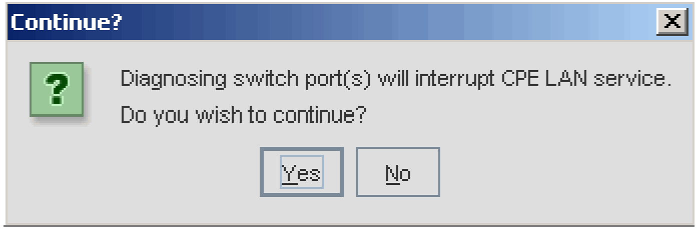
The current status consists of ID, Speed, Status (enabled/disabled), and Connected (true/false). These are polled from the device and updated approximately every 30 seconds while the tab is displayed.

With each port is a “Test” button and a “Test Result” field. The Test buttons can be checked or unchecked to select individual ports for diagnosis. The “All” button is a shortcut to conveniently check or uncheck all interfaces.

The selected ports will be diagnosed when the “Diagnose Interface” button at the bottom of the panel is activated. The operation will take several seconds.

Note: *Testing all interfaces at once will increase the duration of the test and possibly interrupt CPE LAN service, so normally test one interface at a time or small groups at a time rather than all interfaces at one time.*

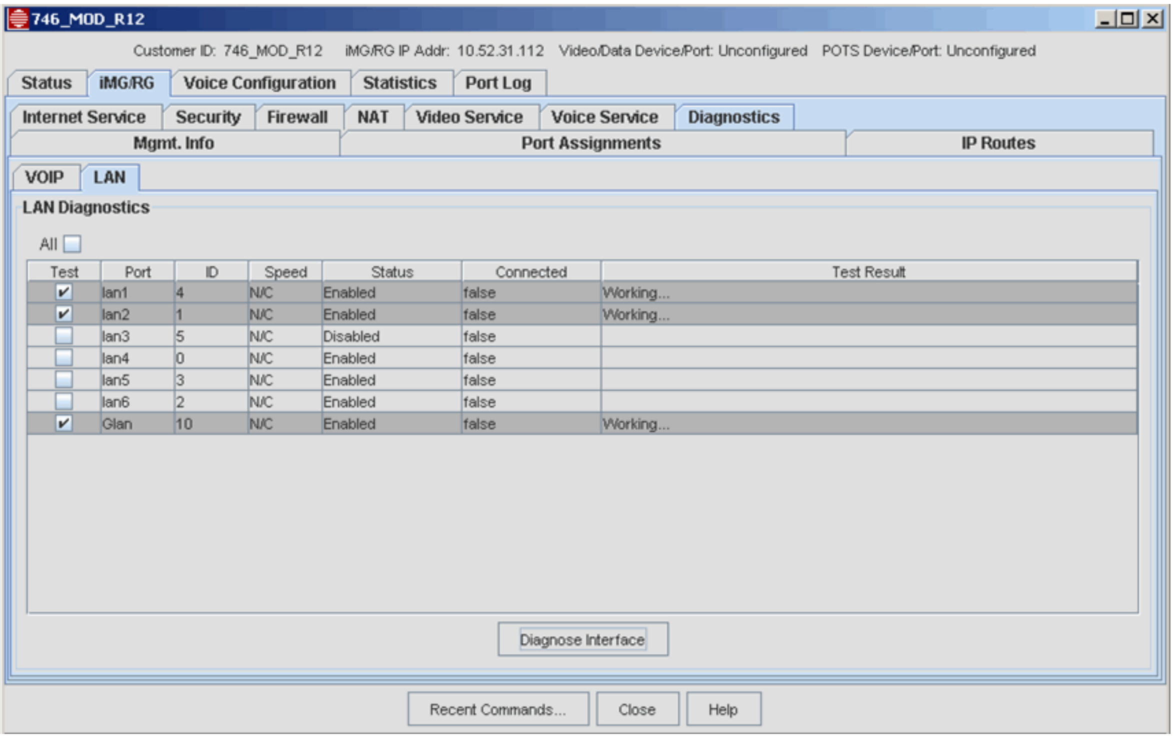
Since CPE LAN service may be interrupted during diagnosis, user confirmation is required before the operation will be performed, as shown in the following figure.



Diagnosing switch port(s) will interrupt CPE LAN service.
Do you wish to continue?

FIGURE 21-126 Warning when Diagnosing LAN Ports

While diagnosis is underway, the test results display “Working” as shown below.



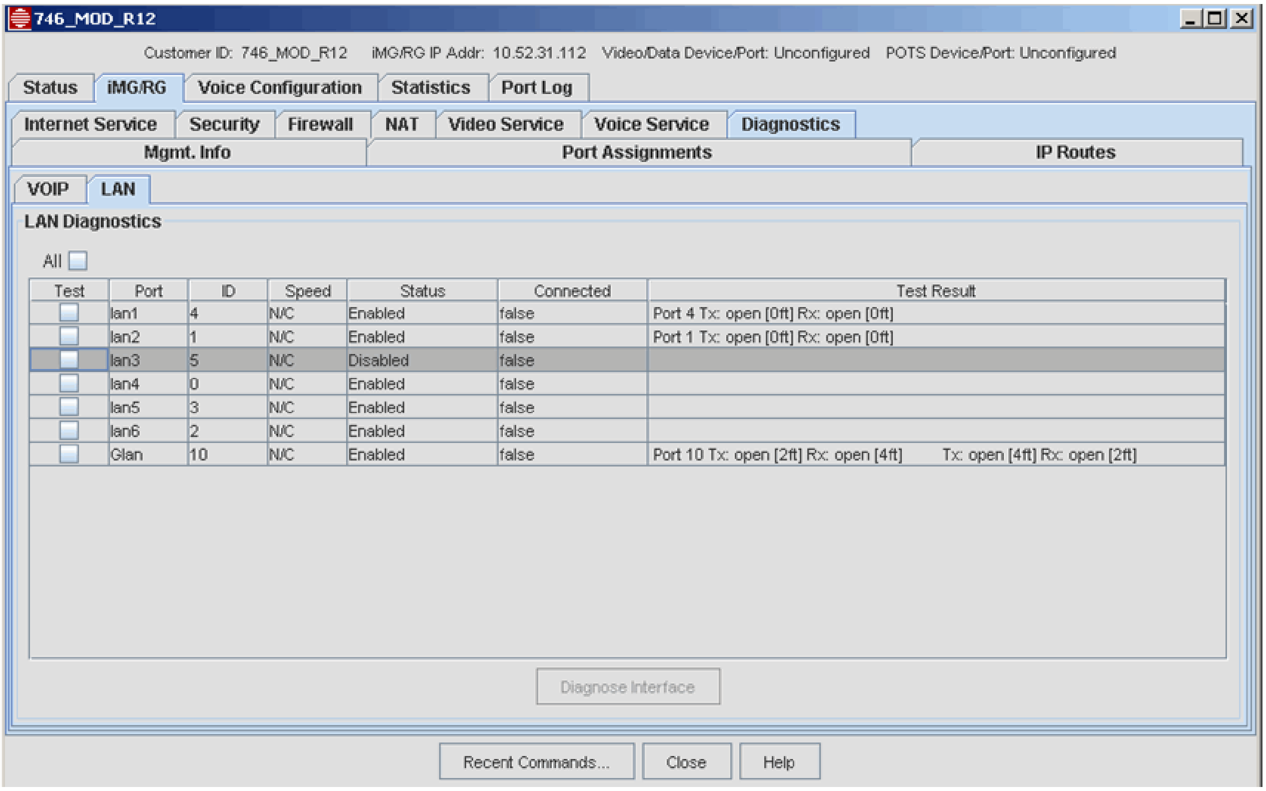
Customer ID: 746_MOD_R12 iMG/RG IP Addr: 10.52.31.112 Video/Data Device/Port: Unconfigured POTS Device/Port: Unconfigured

All □

Test	Port	ID	Speed	Status	Connected	Test Result
☑	lan1	4	N/C	Enabled	false	Working...
☑	lan2	1	N/C	Enabled	false	Working...
□	lan3	5	N/C	Disabled	false	
□	lan4	0	N/C	Enabled	false	
□	lan5	3	N/C	Enabled	false	
□	lan6	2	N/C	Enabled	false	
☑	Glan	10	N/C	Enabled	false	Working...

FIGURE 21-127 LAN Port Diagnostics in Progress

When completed, the results for each interface will be displayed in the Test Result field. Notice the Glan interface, when present, will contain an additional Tx/Rx pair.



Test	Port	ID	Speed	Status	Connected	Test Result
□	lan1	4	N/C	Enabled	false	Port 4 Tx: open [0ft] Rx: open [0ft]
□	lan2	1	N/C	Enabled	false	Port 1 Tx: open [0ft] Rx: open [0ft]
□	lan3	5	N/C	Disabled	false	
□	lan4	0	N/C	Enabled	false	
□	lan5	3	N/C	Enabled	false	
□	lan6	2	N/C	Enabled	false	
□	Glan	10	N/C	Enabled	false	Port 10 Tx: open [2ft] Rx: open [4ft] Tx: open [4ft] Rx: open [2ft]

FIGURE 21-128 LAN Port Diagnostics Complete

For more information on these tests refer to the *ATI Gateway Product Family Software Reference Manual.*

21.20 System Power Management

This feature allows the user to modify power management for the device. When enabled at the device level, specified ports immediately shut down, usually so that services such as lifeline POTS can continue as long as possible on battery backup. When disabled, battery power traps are not sent from the device and port-based power management settings will have no effect.

The table below shows iMG devices running 3.8 indicating which types support the ability to configure system power management or whether the device can display port state for LAN and voice ports.

TABLE 21-15 iMG/RG Power Management Feature and Port State Support

Device Type	System Power Mgmt	LAN Port Power Mgmt	LAN Port State	TEL Ports Power Mgmt	TEL Ports State
RG613-BD/LH	Y				
iMG613-RF	Y				
RG656-BD	Y	Y	Y	Y	Y
iMG606-BD/LH/SH	Y	Y	Y	Y	Y
iMG606-BD-R2	Y	Y	Y	Y	Y
iMG646-BD/LH/SH	Y	Y	Y	Y	Y
iMG646-BD-ON/PX-ON	Y	Y	Y	Y	Y
iMG616-BD/LH/SH	Y				
iMG616-BD-R2	Y				

TABLE 21-15 iMG/RG Power Management Feature and Port State Support

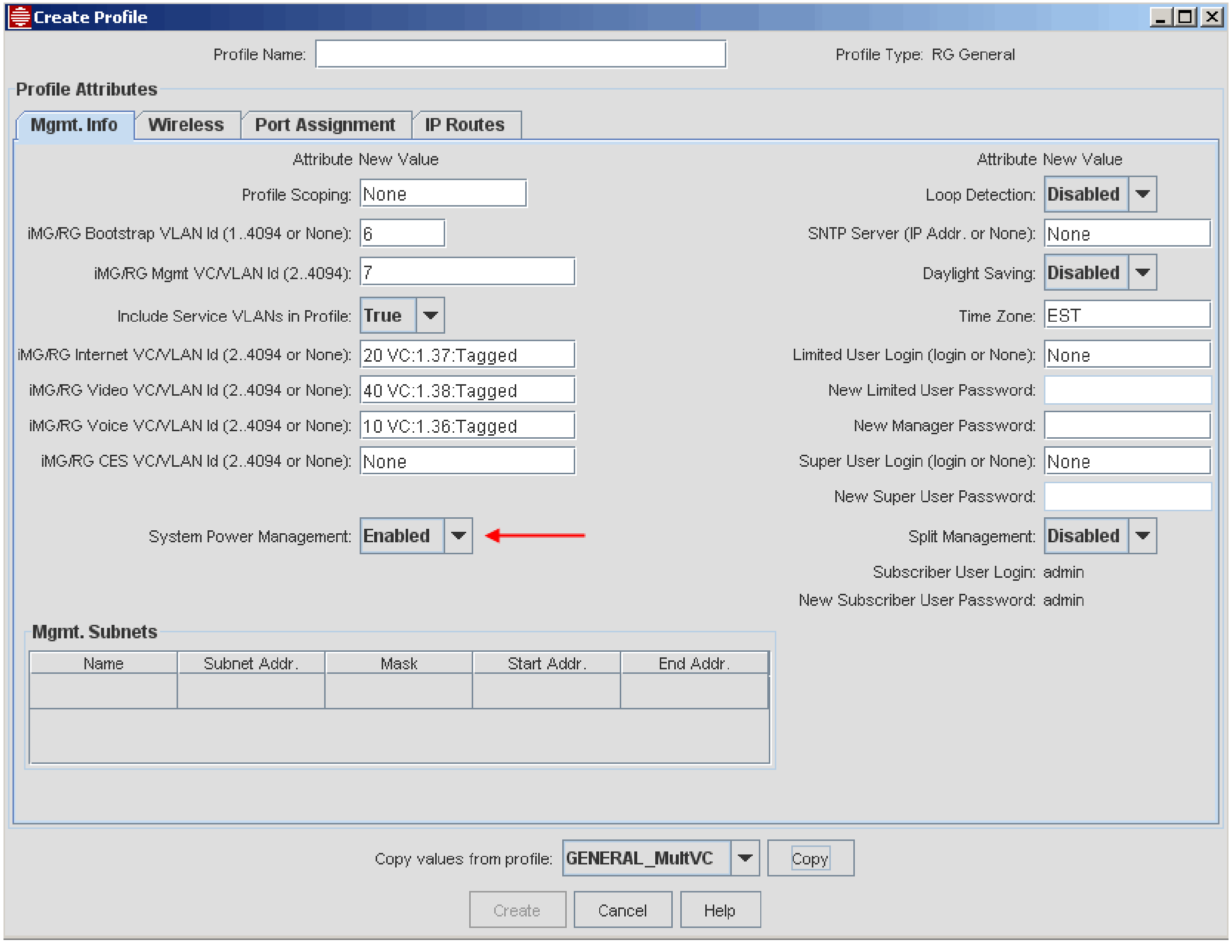
Device Type	System Power Mgmt	LAN Port Power Mgmt	LAN Port State	TEL Ports Power Mgmt	TEL Ports State
iMG616-RF/RF+	Y				
iMG616-SRF+	Y				
iMG616-W	Y	Y	Y	Y	Y
iMG626-MOD	Y	Y	Y	Y	Y
iMG646-MOD	Y	Y	Y	Y	Y
iMG726-MOD	Y	Y	Y	Y	Y
iMG746-MOD	Y	Y	Y	Y	Y
iMG726-BD-ON	Y	Y	Y	Y	Y
iMG624-A	Y				
iMG634-A	Y				
iMG624-A-R2					
iMG634-A-R2					
iMG634-B-R2					
iMG634-WA-R2					
iMG634-WB-R2					
iBG915-FX					

21.20.1 System Power Management

Enabling the feature at the device level is done with the:

- RG General Profile. - Note that the default when creating the profile is Enabled.
- Service Management Form - iMG/RG -> Mgmt Info. (There is also a read-only field that shows the power system status.

Refer to the following figures.



Profile Name:

Profile Type: RG General

Profile Attributes

Attribute	New Value
Profile Scoping:	None
iMG/RG Bootstrap VLAN Id (1..4094 or None):	6
iMG/RG Mgmt VC/VLAN Id (2..4094):	7
Include Service VLANs in Profile:	True
iMG/RG Internet VC/VLAN Id (2..4094 or None):	20 VC:1.37:Tagged
iMG/RG Video VC/VLAN Id (2..4094 or None):	40 VC:1.38:Tagged
iMG/RG Voice VC/VLAN Id (2..4094 or None):	10 VC:1.36:Tagged
iMG/RG CES VC/VLAN Id (2..4094 or None):	None
System Power Management:	Enabled

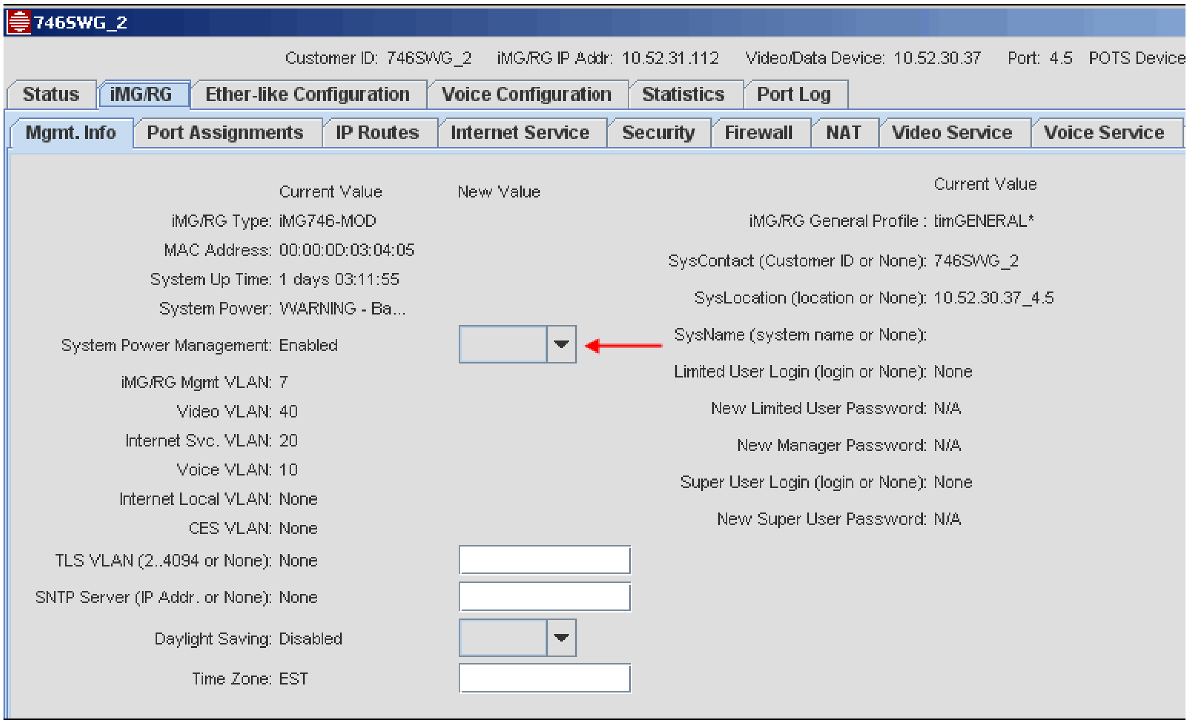
Attribute	New Value
Loop Detection:	Disabled
SNTP Server (IP Addr. or None):	None
Daylight Saving:	Disabled
Time Zone:	EST
Limited User Login (login or None):	None
New Limited User Password:	
New Manager Password:	
Super User Login (login or None):	None
New Super User Password:	
Split Management:	Disabled
Subscriber User Login:	admin
New Subscriber User Password:	admin

Mgmt. Subnets

Name	Subnet Addr.	Mask	Start Addr.	End Addr.

Copy values from profile: GENERAL_MultVC

FIGURE 21-129 System Power Management - RG General Profile



Customer ID: 746SWG_2 iMG/RG IP Addr: 10.52.31.112 Video/Data Device: 10.52.30.37 Port: 4.5 POTS Device

	Current Value	New Value
iMG/RG Type:	iMG746-MOD	
MAC Address:	00:00:0D:03:04:05	
System Up Time:	1 days 03:11:55	
System Power:	WARNING - Ba...	
System Power Management:	Enabled	
iMG/RG Mgmt VLAN:	7	
Video VLAN:	40	
Internet Svc. VLAN:	20	
Voice VLAN:	10	
Internet Local VLAN:	None	
CES VLAN:	None	
TLS VLAN (2..4094 or None):	None	
SNTP Server (IP Addr. or None):	None	
Daylight Saving:	Disabled	
Time Zone:	EST	

	Current Value
iMG/RG General Profile :	timGENERAL*
SysContact (Customer ID or None):	746SWG_2
SysLocation (location or None):	10.52.30.37_4.5
SysName (system name or None):	
Limited User Login (login or None):	None
New Limited User Password:	N/A
New Manager Password:	N/A
Super User Login (login or None):	None
New Super User Password:	N/A

FIGURE 21-130 System Power Management - iMG/RG -> Mgmt. Info

21.20.2 LAN Ports Power Management

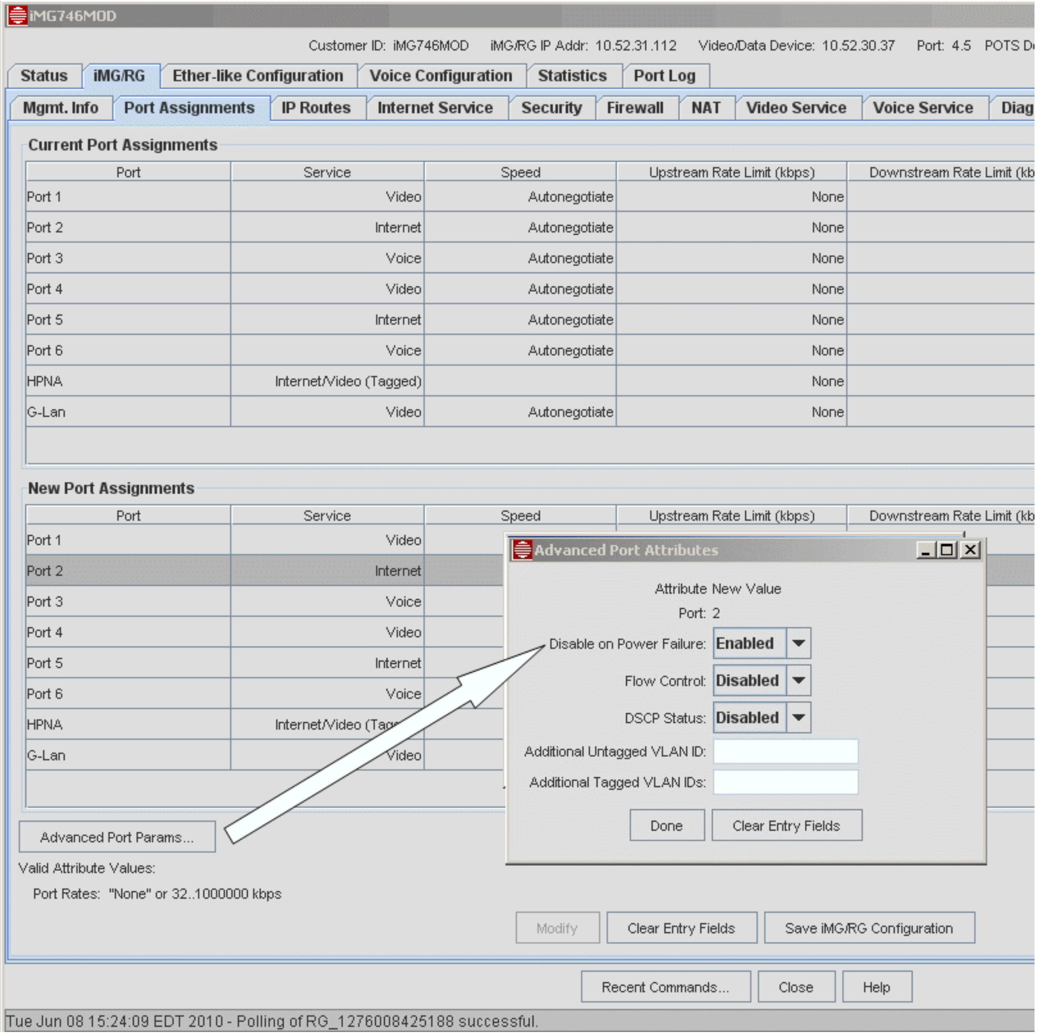
In 3-8, there is also for certain iMG/RGs the ability to configure power management per LAN port, so that a port is automatically disabled in case of power failure. (Before 3-8, some devices had a default setting that of disabling all LAN ports except port 1.) The NMS supports this feature on iMG/RGs as listed in Table 21-15. Refer to the *ATI Gateway Product Family Software Reference Manual* for complete information on this feature and how devices support this feature.

This option is controlled through the Advanced Port Params button on the

- RG General Profile - Refer to iMG General Profile.
- Service Management Form - iMG/RG -> Port Assignments

Note: Disable on Power Failure for CES ports is not supported from the NMS.

The following figure shows the Advanced Port Attributes GUI on the Service Management Form. When Enabled is selected, the port is disabled if there is a power failure.



Customer ID: iMG746MOD iMG/RG IP Addr: 10.52.31.112 Video/Data Device: 10.52.30.37 Port: 4.5 POTS D

Current Port Assignments

Port	Service	Speed	Upstream Rate Limit (kbps)	Downstream Rate Limit (kb
Port 1	Video	Autonegotiate	None	
Port 2	Internet	Autonegotiate	None	
Port 3	Voice	Autonegotiate	None	
Port 4	Video	Autonegotiate	None	
Port 5	Internet	Autonegotiate	None	
Port 6	Voice	Autonegotiate	None	
HPNA	Internet/Video (Tagged)		None	
G-Lan	Video	Autonegotiate	None	

New Port Assignments

Port	Service	Speed	Upstream Rate Limit (kbps)	Downstream Rate Limit (kb
Port 1	Video			
Port 2	Internet			
Port 3	Voice			
Port 4	Video			
Port 5	Internet			
Port 6	Voice			
HPNA	Internet/Video (Ta			
G-Lan	Video			

Advanced Port Attributes

Attribute New Value

Port: 2

Disable on Power Failure: Enabled

Flow Control: Disabled

DSCP Status: Disabled

Additional Untagged VLAN ID:

Additional Tagged VLAN IDs:

Valid Attribute Values:

Port Rates: "None" or 32..1000000 kbps

Tue Jun 08 15:24:09 EDT 2010 - Polling of RG_1276008425188 successful.

FIGURE 21-131 LAN Port Power Management on Service Management Form

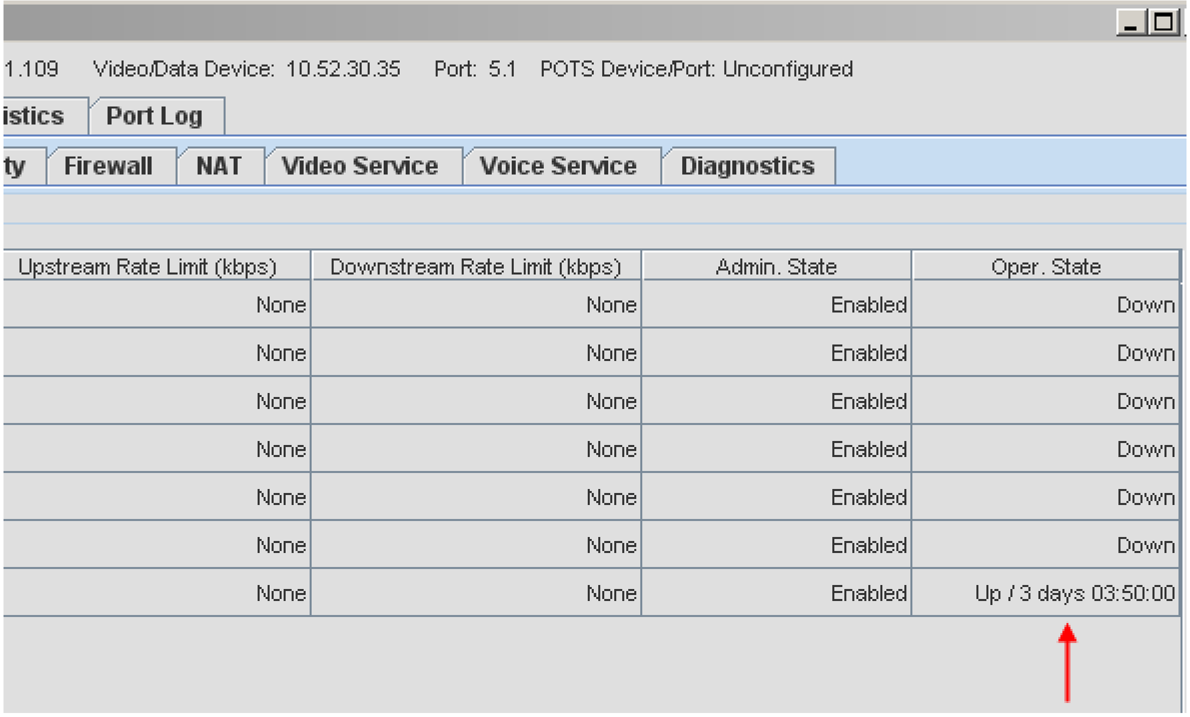
21.20.3 LAN Ports State

In the Service Management Form for iMG/RG -> Port Assignments, the field **Oper. State** shows the state of the port:

- Up - Include the time the link has been active
- Down - The port is out of service because of a problem or it has been disabled.
- Power Down - The port is out of service because of the Port Power Management feature.

Note: The Up state that includes the time applies to all iMG/RGs. The Power Down appears only for the selected iMG/RGs as listed in Table 21-15.

Refer to the following figure.


1.109 Video/Data Device: 10.52.30.35 Port: 5.1 POTS Device/Port: Unconfigured
istics
Port Log
ty
Firewall
NAT
Video Service
Voice Service
Diagnostics

Upstream Rate Limit (kbps)	Downstream Rate Limit (kbps)	Admin. State	Oper. State
None	None	Enabled	Down
None	None	Enabled	Down
None	None	Enabled	Down
None	None	Enabled	Down
None	None	Enabled	Down
None	None	Enabled	Down
None	None	Enabled	Up / 3 days 03:50:00

FIGURE 21-132 Oper.State for Port - Link Up Time

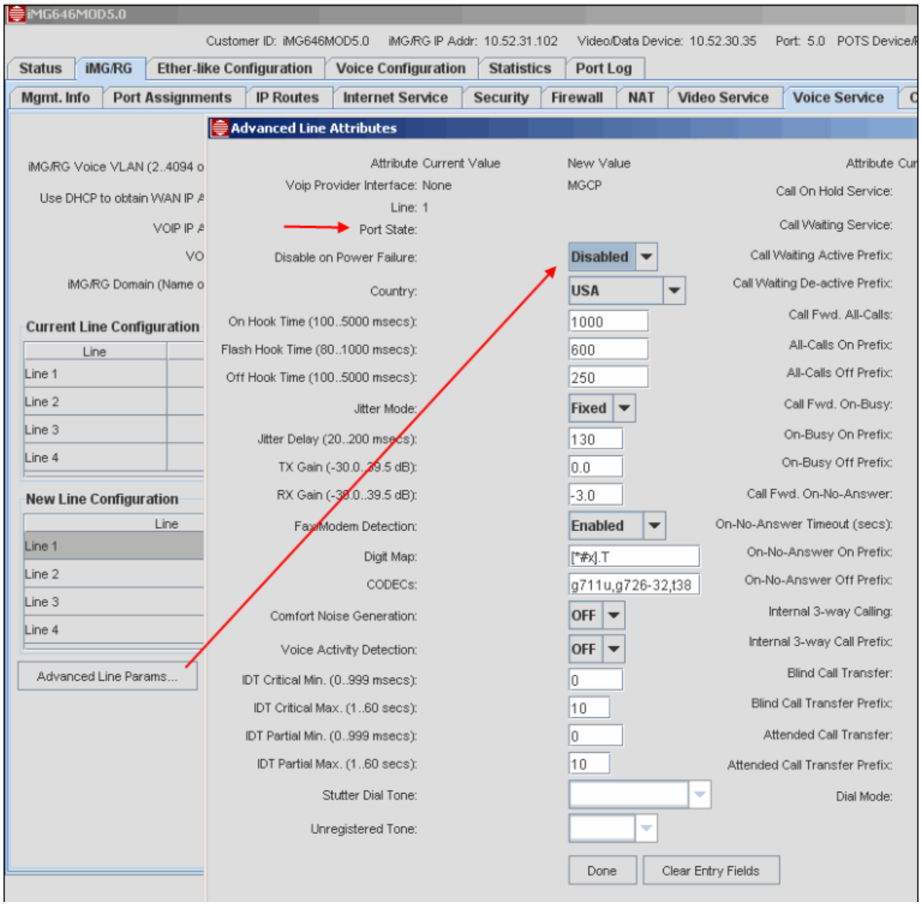
21.20.4 TEL Ports Power Management

In 3-8, there is, similar to the LAN Port Power Management, the ability for certain iMG/RGs the ability to configure power management per voice port, so that a port is automatically disabled in case of power failure. The NMS supports this feature on iMG/RGs as listed in Table 21-15. Refer to the *ATI Gateway Product Family Software Reference Manual* for complete information on this feature and how devices support this feature.

This option is controlled through the Advanced Port Params button on the

- RG Voice Profile - Refer to iMG Voice Profile.
- Service Management Form - iMG/RG -> Voice Service

The following figure shows the Advanced Line Attributes GUI on the Service Management Form.



Customer ID: iMG646MOD5.0 iMG/RG IP Addr: 10.52.31.102 Video/Data Device: 10.52.30.35 Port: 5.0 POTS Device/

Attribute	Current Value	New Value
Voip Provider Interface:	None	MGCP
Line:	1	
Port State:		
Disable on Power Failure:		Disabled
Country:		USA
On Hook Time (100..5000 msecs):		1000
Flash Hook Time (80..1000 msecs):		600
Off Hook Time (100..5000 msecs):		250
Jitter Mode:		Fixed
Jitter Delay (20..200 msecs):		130
TX Gain (-30.0..39.5 dB):		0.0
RX Gain (-30.0..39.5 dB):		-3.0
Fax/Modem Detection:		Enabled
Digit Map:		[*#x].T
CODECs:		g711u,g726-32,t38
Comfort Noise Generation:		OFF
Voice Activity Detection:		OFF
IDT Critical Min. (0..999 msecs):		0
IDT Critical Max. (1..60 secs):		10
IDT Partial Min. (0..999 msecs):		0
IDT Partial Max. (1..60 secs):		10

FIGURE 21-133 Controlling power Management for Voice Lines on Service Management Form

21.20.5 Voice Ports State

Also on the Advanced Line Params for voice service is a read-only field that shows the state of the port:

- Busy - The line is being used. Note that during this state, it cannot be powered down by the Power Management feature if there is a loss of power.
- Idle - Line is ready to place and receive calls.
- Out of Service - Line has been disabled.
- Powered Down - The Power Management Feature has activated and on the voice port the Disable on Power Failure was set to Enabled.

This status field can be seen on Figure 21-133.

21.21 Flow Control

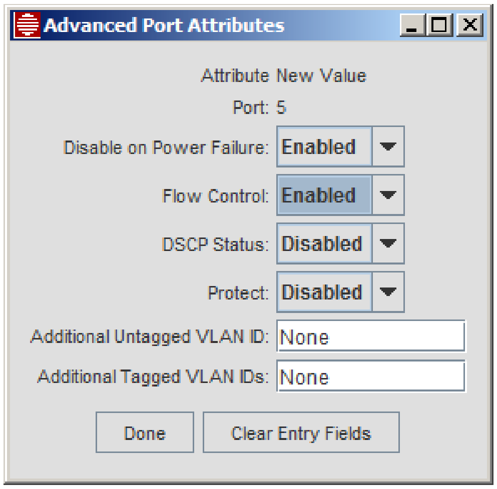
Flow control allows you to control traffic rates by temporarily suspending data packet transmission when a network is congested. When an ingress queue is full and cannot receive any more traffic, flow control causes the iMG to send a pause frame for all traffic on the port. When a remote device receives the pause frame it should stop sending data packets to the port to ensure traffic is not lost while the port is congested.

You can enable flow control on a new profile, an existing profile, or on an existing device.

21.21.1 Enabling Flow Control in a New Profile

To enable flow control in a new profile:

1. In the **Network Objects** panel, go to **Network Service Data** > **Profiles**.
2. From the menu, go to **Network Services** > **Profile** > **iMG/RG Service Profiles** > **Create iMG/RG General Profile**. The **Create Profile** box for the RG General profile appears.
3. In the **Profile Name** field, enter a name for the profile.
4. Select the **Port Assignment** tab.
5. Under **PortAssignments**, select the port you want to configure.
6. In the **Admin. State** column, select **Enabled** in the drop-down list to enable the port. The port must be enabled to configure advanced parameters.
7. Click **Advanced Port Params....** The **Advanced Port Attributes** box appears.
8. In the **Flow Control** drop-down list, select **Enabled**.



Attribute New Value
Port: 5
Disable on Power Failure: Enabled
Flow Control: Enabled
DSCP Status: Disabled
Protect: Disabled
Additional Untagged VLAN ID: None
Additional Tagged VLAN IDs: None

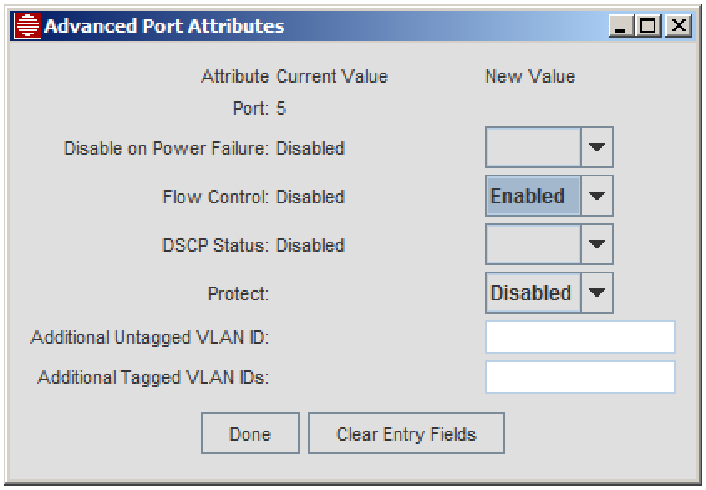
FIGURE 21-134 Advanced Port Attributes - Flow Control

9. Make any other selections for the profile.
10. Click **Done**, then click **Create** to save the profile.

21.21.2 Enabling Flow Control in an Existing Profile

To enable flow control in an existing profile:

1. In the **Network Objects** panel, go to **Network Service Data > Profiles**.
2. In the **Profiles** window, select the RG General profile you want to modify.
3. Right-click, then select **View Profile**. The **Modify Profile** box appears.
4. Select the **Port Assignment** tab.
5. Under **New Port Assignments**, select the port you want to modify.
6. Click **Advanced Port Params....** The **Advanced Port Attributes** box appears.
7. In the **Flow Control** drop-down list, select **Enabled**.



Attribute Current Value New Value

Port: 5

Disable on Power Failure: Disabled

Flow Control: Disabled Enabled

DSCP Status: Disabled

Protect: Disabled

Additional Untagged VLAN ID:

Additional Tagged VLAN IDs:

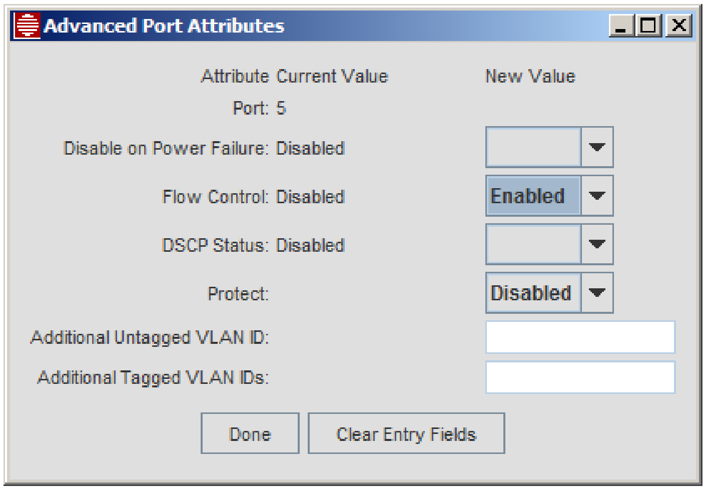
FIGURE 21-135 Advanced Port Attributes - Flow Control

8. Click **Done**, then click **Modify** to save the changes to the profile.

21.21.3 Enabling Flow Control on an Existing Device

To enable flow control in an existing device:

1. In the **Network Objects** panel, go to **Network Inventory** > **iMG/RGs**.
2. In the **iMG/RGs** window, select the device you want to modify.
3. Right-click, then select **View/Modify Details**. The device's settings window appears.
4. Select the **iMG/RG** tab.
5. Select the **Port Assignments** tab.
6. Under **New Port Assignments**, select the port you want to modify.
7. Click **Advanced Port Params...**. The **Advanced Port Attributes** box appears.
8. In the **Flow Control** drop-down list, select **Enabled**.



Attribute Current Value New Value

Port: 5

Disable on Power Failure: Disabled

Flow Control: Disabled Enabled

DSCP Status: Disabled

Protect: Disabled

Additional Untagged VLAN ID:

Additional Tagged VLAN IDs:

FIGURE 21-136 Advanced Port Attributes - Flow Control

9. Click **Done**, then click **Modify** to save the changes to the device.

21.22 Protected Ports

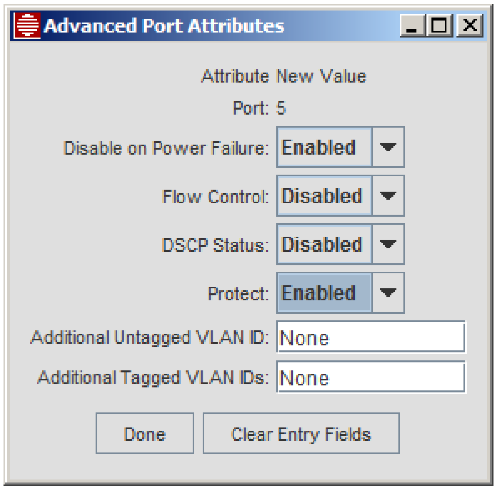
You can designate LAN ports (ports 1-6) as protected on iMG 1000 and iMG 2000 series devices. A protected port is isolated from other local ports and cannot receive traffic from the other ports. If you have multiple subscribers utilizing a single iMG, protecting the ports prevents a subscriber from receiving feeds intended for someone else.

You can enable protected ports on a new profile, an existing profile, or on an existing device.

21.22.1 Enabling Protected Ports in a New Profile

To enable protected ports in a new profile:

1. In the **Network Objects** panel, go to **Network Service Data** > **Profiles**.
2. From the menu, go to **Network Services** > **Profile** > **iMG/RG Service Profiles** > **Create iMG/RG General Profile**. The **Create Profile** box for the RG General profile appears.
3. In the **Profile Name** field, enter a name for the profile.
4. Select the **Port Assignment** tab.
5. Under **PortAssignments**, select the LAN port (ports 1-6) you want to configure.
6. In the **Admin. State** column, select **Enabled** in the drop-down list to enable the port. The port must be enabled to configure advanced parameters.
7. Click **Advanced Port Params...**. The **Advanced Port Attributes** box appears.
8. In the **Protect** drop-down list, select **Enabled**.



Attribute New Value
Port: 5
Disable on Power Failure: Enabled
Flow Control: Disabled
DSCP Status: Disabled
Protect: Enabled
Additional Untagged VLAN ID: None
Additional Tagged VLAN IDs: None

FIGURE 21-137 Advanced Port Attributes - Protected Ports

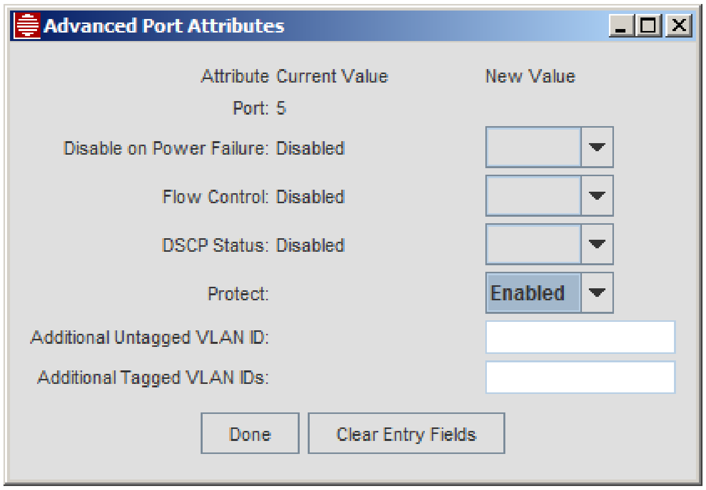
9. Make any other selections for the profile.
10. Click **Done**, then click **Create** to save the profile.

21.22.2 Enabling Protected Ports in an Existing Profile

To enable protected ports in an existing profile:

1. In the **Network Objects** panel, go to **Network Service Data > Profiles**.
2. In the **Profiles** window, select the profile you want to modify.
3. Right-click, then select **View Profile**. The **Modify Profile** box appears.
4. Select the **Port Assignment** tab.
5. Under **New Port Assignments**, select the LAN port (ports 1-6) you want to modify.

6. Click **Advanced Port Params...**. The **Advanced Port Attributes** box appears.
7. In the **Protect** drop-down list, select **Enabled**.



Attribute Current Value New Value

Port: 5

Disable on Power Failure: Disabled

Flow Control: Disabled

DSCP Status: Disabled

Protect: Enabled

Additional Untagged VLAN ID:

Additional Tagged VLAN IDs:

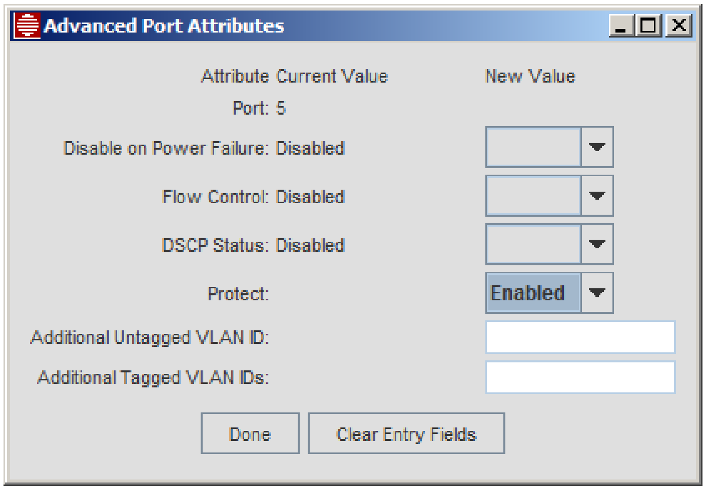
FIGURE 21-138 Advanced Port Attributes - Protected Ports

8. Click **Done**, then click **Modify** to save the changes to the profile.

21.22.3 Enabling Protected Ports on an Existing Device

To enable protected ports in an existing device:

1. In the **Network Objects** panel, go to **Network Inventory** > **iMG/RGs**.
2. In the **iMG/RGs** window, select the device you want to modify.
3. Right-click, then select **View/Modify Details**. The device's settings window appears.
4. Select the **iMG/RG** tab.
5. Select the **Port Assignments** tab.
6. Under **New Port Assignments**, select the LAN port (ports 1-6) you want to modify.
7. Click **Advanced Port Params...**. The **Advanced Port Attributes** box appears.
8. In the **Protect** drop-down list, select **Enabled**.



Attribute Current Value New Value

Port: 5

Disable on Power Failure: Disabled

Flow Control: Disabled

DSCP Status: Disabled

Protect: Enabled

Additional Untagged VLAN ID:

Additional Tagged VLAN IDs:

FIGURE 21-139 Advanced Port Attributes - Protected Ports

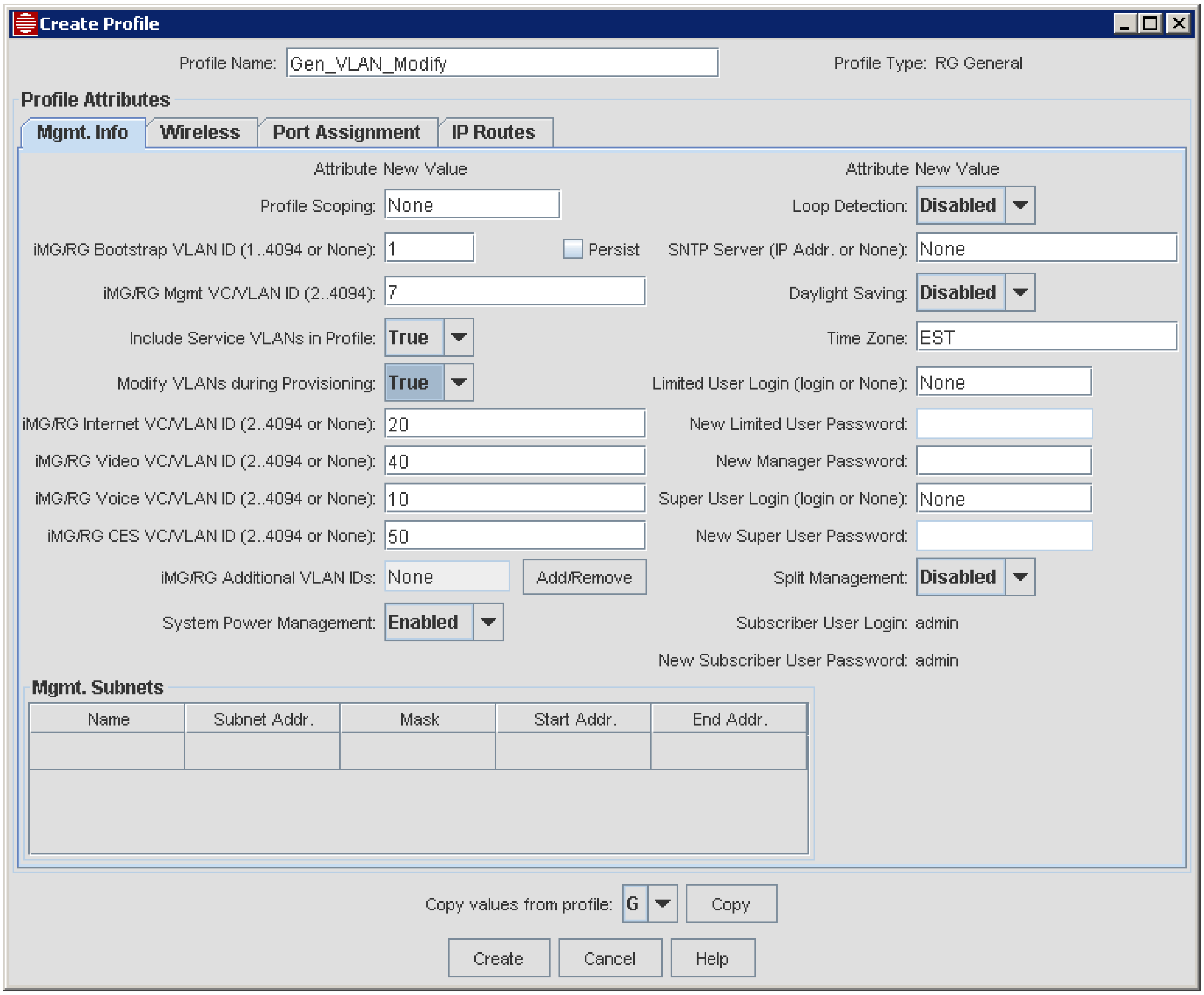
9. Click **Done**, then click **Modify** to save the changes to the device.

21.23 Assigning Customer-Specific VLAN IDs to iMGs

When you use profiles to provision iMGs for triple play, you can modify VLANs during provisioning to set customer-specific VLANs on the iMGs. The iMGs can then connect to customer-specific HVLANs on the switch.

To modify VLANs during provisioning:

1. In the **Network Objects** panel, go to **Network Service Data** > **Profiles**.
2. From the menu, go to **Network Services** > **Profile** > **iMG/RG Service Profiles** > **Create iMG/RG General Profile**. The **Create Profile** box for the RG General profile appears.
3. In the **Profile Name** field, enter a name for the profile.
4. If it is not already selected, select the **Mgmt. Info** tab.
5. In the **Modify VLANs during Provisioning** drop-down list, select **True**. This enables fields on the Triple Play form that allow you to supply customer-specific VLAN IDs.
6. To pre-populate the Triple Play form fields with the default VLAN IDs, in the **Include Service VLANs in Profile** drop-down list, select **True**. If you set **Include Service VLANs in Profile** to **False**, the Triple Play form fields will be blank and require a value.



Profile Name: Gen_VLAN_Modify
Profile Type: RG General

Profile Scoping: None
iMG/RG Bootstrap VLAN ID (1..4094 or None): 1 □ Persist
iMG/RG Mgmt VC/VLAN ID (2..4094): 7
Include Service VLANs in Profile: True
Modify VLANs during Provisioning: True
iMG/RG Internet VC/VLAN ID (2..4094 or None): 20
iMG/RG Video VC/VLAN ID (2..4094 or None): 40
iMG/RG Voice VC/VLAN ID (2..4094 or None): 10
iMG/RG CES VC/VLAN ID (2..4094 or None): 50
iMG/RG Additional VLAN IDs: None
System Power Management: Enabled

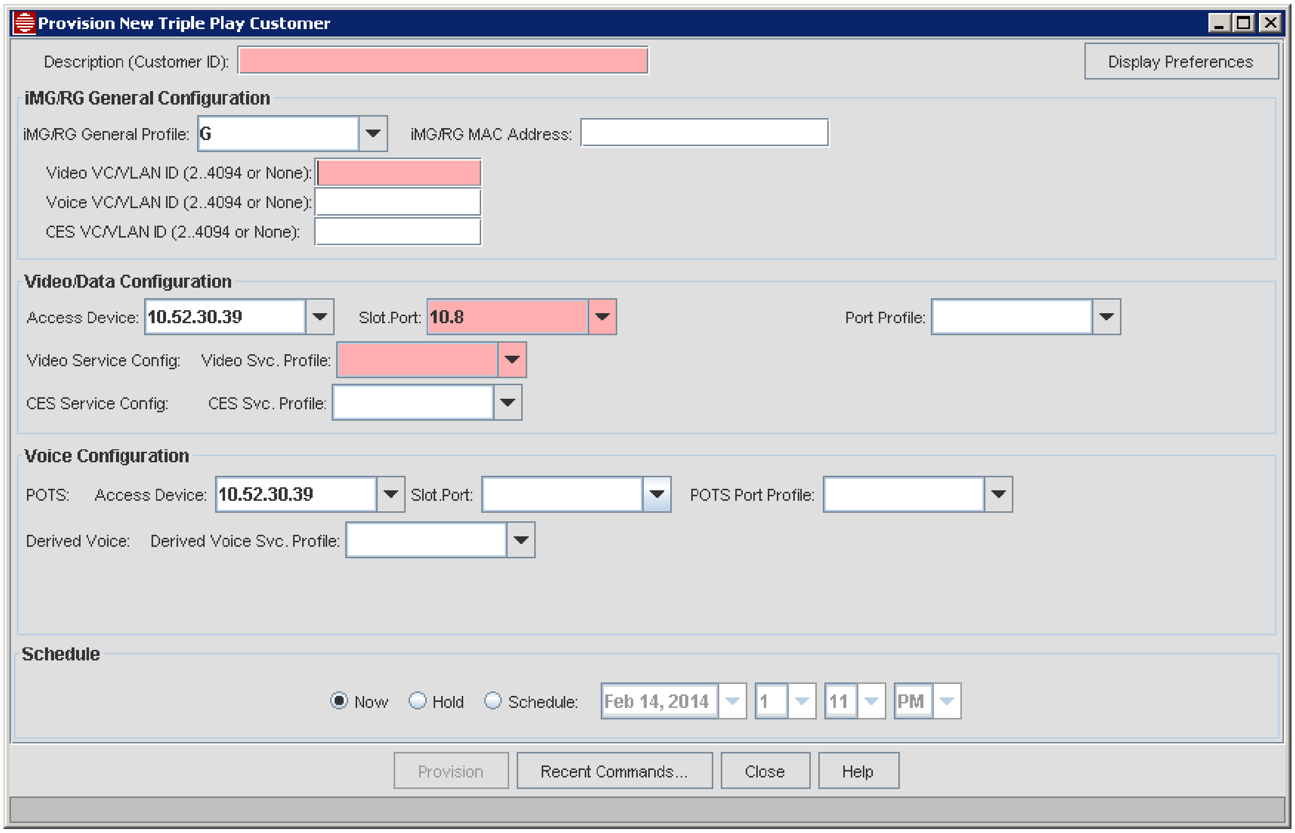
Loop Detection: Disabled
SNTP Server (IP Addr. or None): None
Daylight Saving: Disabled
Time Zone: EST
Limited User Login (login or None): None
New Limited User Password:
New Manager Password:
Super User Login (login or None): None
New Super User Password:
Split Management: Disabled
Subscriber User Login: admin
New Subscriber User Password: admin

Name	Subnet Addr.	Mask	Start Addr.	End Addr.

Copy values from profile: G

FIGURE 21-140 General Profile - Modify VLANs during Provisioning

7. Click **Create** to save the profile.
8. In the **Network Objects** panel, go to **Network Inventory > iMG/RGs**. Select the iMG you want to configure.
9. Right-click, then select **Provision New Customer/iMG/RG**. The **Provision New Triple Play Customer** box appears.
10. In the **iMG/RG General Profile** drop-down list, select the general profile you created. The **VC/VLAN ID (2.. 4094 or None)** fields appear. The VC/VLAN ID fields that appear as required depend on the on the port assignments you make in the Port Assignment Tab.


Provision New Triple Play Customer

Description (Customer ID):

iMG/RG General Configuration

iMG/RG General Profile: G

iMG/RG MAC Address:

Video VC/VLAN ID (2..4094 or None):

Voice VC/VLAN ID (2..4094 or None):

CES VC/VLAN ID (2..4094 or None):

Video/Data Configuration

Access Device: 10.52.30.39 Slot.Port: 10.8 Port Profile:

Video Service Config: Video Svc. Profile:

CES Service Config: CES Svc. Profile:

Voice Configuration

POTS: Access Device: 10.52.30.39 Slot.Port: POTS Port Profile:

Derived Voice: Derived Voice Svc. Profile:

Schedule

● Now ○ Hold ○ Schedule: Feb 14, 2014 1 11 PM

FIGURE 21-141 Triple Play Form with VLAN Fields Enabled

11. In the **VC/VLAN ID (2.. 4094 or None)** fields, enter the customer-specific VLAN IDs.
12. Click **Provision** to provision the customer.

21.23.1 Profile Dependencies

iMG profiles are interdependent. When you set **Modify VLANs during Provisioning** to **True** in a general profile, you must set fields in the service and port profiles to **False**. Table 21-16 lists the dependencies between the profiles and the required field settings.

TABLE 21-16 **Profile Dependencies for Modifying VLANs During Provisioning**

Profile	Tab	Field	Value
iMG General Profile	Mgmt. Info Tab	Modifying VLANs during Provisioning	True
iMG General Profile	Mgmt. Info Tab	Include Service VLANs in Profile	True or False If True, VLAN ID fields on the Triple Play form will be pre-populated with default values. If False, VLAN ID fields on the Triple Play form will be blank and require a value.
iMG Internet Profile	General Internet Info Tab	Include Internet VLAN in Profile	False
iMG Video Profile	General Video Info Tab	Include Video VLAN in Profile	False
iMG Voice Profile	General Voice Info Tab	Include Voice VLAN in Profile	False
Etherlike Port Profile	Common Tab	Include VLAN Configuration in Profile	False

21.24 Port-Based Rate Limiting

Following are the rules and tables to use to select port-based rate limiting for the iMG/RG for that include release 3-7. The settings that are possible depend on the type of iMG/RG and the software release that the device is using. The following table lists the device types and loads supported. Refer to this table when reviewing the rate limits.

Note: *A value of 0 disables the tx or rx ratelimiting function.*

Note: *Careful consideration must be given during the creation/planning of the iMG/RG General Profiles which establish the setting for ratelimiting. Otherwise you may get an alarm indicating a device's settings are out of sync with the applied profile every rediscovery period. This will most likely happen if you created a profile setup with rate limiting setting for a one iMG/RG type (such as an iMG646) and you apply the profile to a different type that has different rate settings. This is why the administrator is advised to create profile names that minimize confusion.*

Note: *If these values are not input, the rate rounds down to the next available rate.*

TABLE 21-17 **Functional Groupings of iMG/RG**

Group	Model	Load Name	Characteristics	Uniqueness
Fiber A	rg613TX, BD, LH, SH	rg600E	4/16 Meg Flash/Ram	Initial product offering
	rg623TX, BD, LH, SH		Kendin Switch	
			Ni-210 Processor	
Fiber B	rg656BD, LH, SH	RG6x6E	4/16 Meg Flash/Ram	More efficient routing when VLANs configured.Similar service offering to Modular Devices
	iMG606BD, LH, SH		Broadcom Switch	
	iMG646BD, LH, SH		Ni-210 Processor	
	iMG646BD-ON/PX-ON			

TABLE 21-17 Functional Groupings of iMG/RG (Continued)

Group	Model	Load Name	Characteristics	Uniqueness
Fiber C	iMG616BD, LH, SH	iMG616E	4/16 Meg Flash/Ram	Base Platform that provides capability for RF overlay.
	iMG616RF, RF+,		Broadcom Switch	
	iMG616SRF, SRF+		Ni-210 Processor	
Fiber D	iMG616W	iMG616W	8/32 Meg Flash/RAM	New indoor wireless product - greater processing capacity - and wireless support
	iMG606BD-R2	iMG606BD-R2	Broadcom Switch	
	iMG616BD-R2	iMG616BD-R2	Solos Processor	
Fiber E	iBG915FX	iBG915	8/32 Meg Flash/RAM	New Multi port Tel port offering. SFP provides for WAN flexibility.
			Marvell Switch	
			He-520 Processor	
Modular	iMG626MOD	iMG626	8/32 Meg Flash/RAM	Modular outdoor devices - provide support for different WAN services - and additional LAN interfaces.
	iMG646MOD	iMG646	Marvell Switch	
	iMG726MOD	iMG726	He-520 Processor	
	iMG746MOD	iMG746		
	iMG726BD-ON	iMG726	(non-modular)	
ADSL A	iMG624A/B	iMG624A/B	8/32 Meg Flash/RAM	Second Generation ADSL CPE.
	iMG634A/B	iMG634A/B	Kendin Switch	
	iMG634WA/B	iMG634A/B	Argon Processor	
ADSL B	iMG624A-R2	iMG624A-R2	8/32 Meg Flash/RAM	Third Generation ADSL CPE - Greater performance - able to support 2 INP.
	iMG634A/B-R2	iMG634A/B-R2	Marvell Switch	
	iMG634WA/WB-R2	iMG634WA/ WB-R2	Solos Processor	
ADSL C (no NMS support)	iBG910A/B	iBG910A/B	8/32 Meg Flash/RAM	Multi-line ADSL Gateway supporting both ISDN and POTS.
			Marvell Switch	
			Argon Processor	

TABLE 21-18 Port Rate Limits - Rules (Based on Functional Group)

Group	Rule / Load	Range
Fiber A	Same as 3-5	
Fiber B	Broadcom based	None | 128Kbps | 256Kbps | 512Kbps | 756Kbps | 1Mbps | 1.5Mbps | 2Mbps | 3Mbps | 4Mbps | 5Mbps | 6Mbps | 7Mbps | 8Mbps | 9Mbps | 10Mbps | 12Mbps | 14Mbps | 16Mbps | 18Mbps | 20Mbps | 25Mbps | 30Mbps | 35Mbps | 40Mbps | 45Mbps | 50Mbps | 60Mbps | 70Mbps | 80Mbps | 90Mbps
Fiber C	Broadcom based	0 to 1792 Kbps in 64K increments, then 2000 to 12000 in 1Mbps increments
Fiber D	Broadcom based	Refer to Fiber B
Fiber E	Marvell based	None | 128Kbps | 256Kbps | 512Kbps | 1Mbps | 2Mbps | 4Mbps | 8Mbps
Modular	Marvell based	For iMG626MOD and iMG646MOD, refer to Fiber E For iMG726MOD and iMG746MOD, refer to Fiber B [1]
ADSL A	Kendin based	0 to 12000 in 32Kbps increments

TABLE 21-18 Port Rate Limits - Rules (Based on Functional Group)

Group	Rule / Load	Range
ADSL B	Marvell based	Refer to Fiber E
ADSL C	Marvell based	Refer to Fiber E

[1] With Copper Gig Port, can go above 100Mbps.

22. Provisioning the iMG7x6MOD

This type of iMG is highlighted because of the flexibility in provisioning both the WAN and LAN cards. Refer to the following figure.

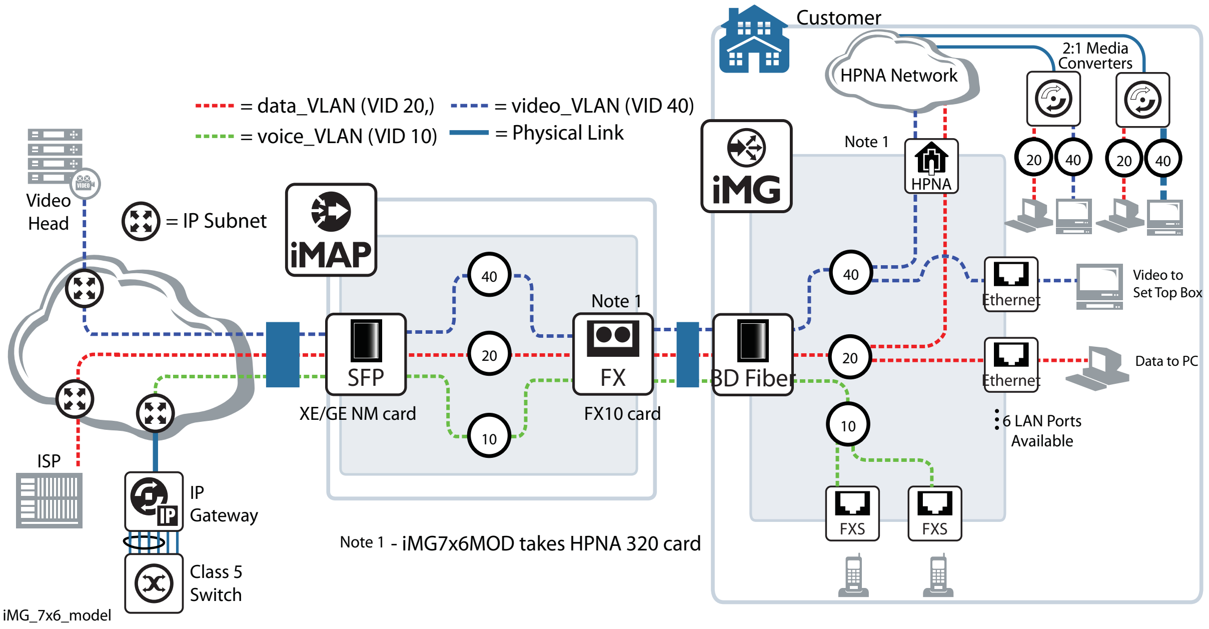


FIGURE 22-1 iMG7x6MOD Configuration

23. Managing Wireless Routers on an iMG

The NMS allows you to manage wireless routers as subtended devices attached to a LAN port on an iMG. Wireless routers act as a wireless access point, extending subscribers' private network capabilities.

The NMS supports the following wireless routers:

- AT-WR2304N

Figure 23-1 illustrates the position of a wireless router in a network.

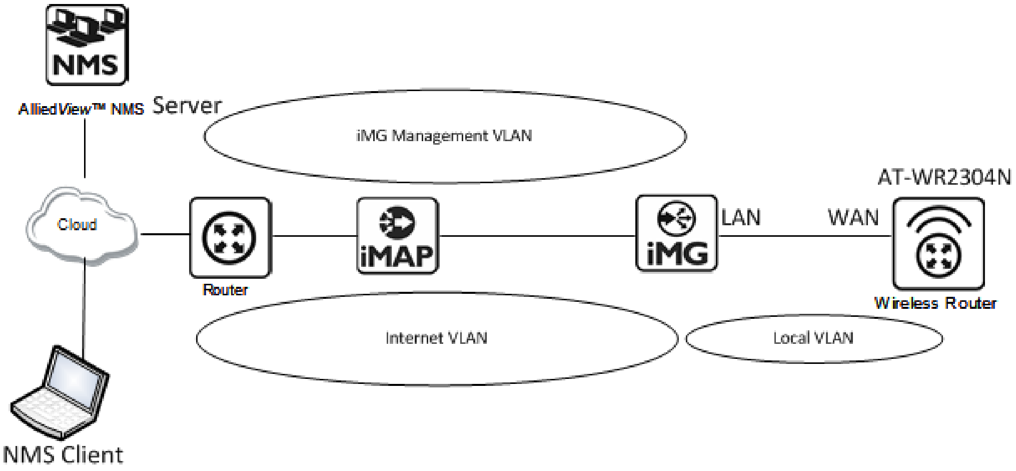


FIGURE 23-1 AT-WR2304N subtended off an iMG

23.1 System Requirements

TABLE 23-1 System Requirements for Managing Wireless Routers

Device	Software Release
iMG 1000 or iMG 2000 series device	4.3.3 or higher
AT-WR2304N	1.2.0.10 or higher **Note:** If you are upgrading to a supported version, you must upgrade both the kernel and the application firmware on the device.

23.2 Overview of the AT-WR2304N Wireless Router Solution

The NMS manages wireless routers by providing an unsecure tunnel into a customer's firewall, then opening the wireless router's management web page in a browser. The NMS configures the NAT rules on the iMG to set up a port forwarding service. The forwarding service directs traffic to the iMG's Internet interface and the configured external port number to the private management IP address and default web server port of the wireless router.

By default, the NMS uses 5080 for the first external port and increments the port by one for each additional device. The NMS uses 80 for the internal port. You can modify these settings if necessary.

When the NMS opens the tunnel, a dialog box opens to control the process and associate the tunnel in the iMG with the management session. The **Close When Finished** dialog box also serves as a reminder that the tunnel through the iMG is not secure and should only remain open while you are actively browsing to the wireless router. While the tunnel is open you cannot perform any other task in the NMS on the iMG screen. When you close the dialog box, the NMS terminates the connection with the wireless router web page and removes the tunnel from the iMG.

Configuring a wireless router to be managed by the NMS requires the following four procedures:

- Provisioning the iMG
- Configuring the AT-WR2304N Wireless Router
- Connecting the AT-WR2304N Wireless Router to the iMG
- Browsing to the Wireless Router from the NMS

23.2.1 Rules and Restrictions

The following rules apply to the wireless router solution:

- The iMG must be configured as routed and have NAT enabled.
- You must use a remote NMS client to connect to a wireless router through an iMG, not the client on the NMS server. The iMG maintains a static route to the NMS server on the management VLAN, preventing a connection to the router.

23.3 Provisioning the iMG

Provisioning the iMG involves three steps:

- Creating the iMG General Profile
- Creating the iMG Internet Profile
- Provisioning a New Triple Play Customer

Table 23-2 summarizes the required settings for the iMG General and Internet profiles.

TABLE 23-2 **iMG Profile Settings for Managing a Wireless Router from the NMS**

iMG Profile	Tab	Field	Value
General	Port Assignment	Service (for the specified port)	Internet or Internet/Video
	IP Routes	All columns	Ensure there are no routes with the subnet of the NMS client machine. Routes with the NMS client machine subnet may prevent browsing to the wireless router from the NMS client.
Internet	General Internet Info	Internet Service Type	Routed Service
	Security	Security	Enabled
	NAT	NAT	Enabled

23.3.1 Creating the iMG General Profile

This section describes how to configure the General profile settings required to manage a wireless router from the NMS. For a description of all settings available in the General profile, see iMG General Profile.

1. In the **Network Objects** panel, go to **Network Service Data** > **Profiles**.
2. From the menu, go to **Network Services** > **Profile** > **iMG/RG Service Profiles** > **Create iMG/RG General Profile**. The **Create Profile** box for the RG General profile appears.
3. In the **Profile Name** field, enter a name for the profile.
4. Select the **Port Assignment** tab.
5. Select a port that will have a wireless router connected to it.
6. In the **Service** drop-down list, select **Internet** or **Internet/Video**.
7. Select the **IP Routes** tab. Ensure there are no routes with the subnet of the NMS client machine.
8. Click **Create** to save the profile.

23.3.2 Creating the iMG Internet Profile

This section describes how to configure the Internet profile settings required to manage a wireless router from the NMS. For a description of all settings available in the Internet profile, see iMG Internet Profile.

1. In the **Network Objects** panel, go to **Network Service Data** > **Profiles**.
2. From the menu, go to **Network Services** > **Profile** > **iMG/RG Service Profiles** > **Create iMG/RG Internet Profile**. The **Create Profile** box for the RG Internet profile appears.
3. In the **Profile Name** field, enter a name for the profile.
4. On the **General Internet Info** tab, in the **Internet Service Type** drop-down list, select **Routed Service**.
5. Select the **Security** tab. In the **Security** drop-down list, select **Enabled**.
6. Select the NAT tab. In the **NAT** drop-down list, select **Enabled**.
7. Click **Create** to save the profile.

23.3.3 Provisioning a New Triple Play Customer

1. Install and power on the iMG.
2. In the **Network Objects** panel, go to **Network Inventory > iMG/RGs**.
3. In the iMG/RGs panel, select the iMG.
4. From the menu, go to **Network Operations > Provision New Customer/iMG/RG**. The **Provision New Triple Play Customer** box appears.
5. In the Description (Customer ID) field, enter a name for the customer. See Naming Convention for Customer IDs (Triple Play Form) for information on naming conventions.
6. In the **iMG/RG General Profile** drop-down list, select the General profile you created.
7. In the **Internet Svc. Profile** drop-down list, select the Internet profile you created.
8. Click **Provision** to provision the iMG.

23.4 Configuring the AT-WR2304N Wireless Router

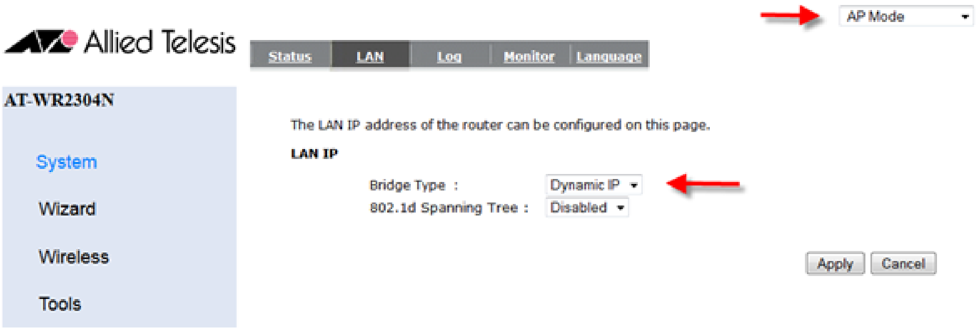
This section describes the settings required on the wireless router to allow it to be managed from the NMS. For complete instructions on how to configure the AT-WR2304N wireless router, see the *AT-WR2304N User Manual* available on the Allied Telesis web site at www.alliedtelesis.com/.

1. Power on the wireless router.
2. Connect a computer to the wireless router’s LAN port.

3. Open a browser and browse to http://192.168.1.1, then log into the device. The default username and password are:

   username: manager
   password: friend

4. In the drop-down list in the upper right corner of the screen, select **AP Mode**.
5. In the pop-up box that appears, click **OK** to restart the system.
6. On the **System** page, select the **LAN** tab.
7. In the **Bridge Type** drop-down list, select **Dynamic IP**.



The LAN IP address of the router can be configured on this page.

LAN IP

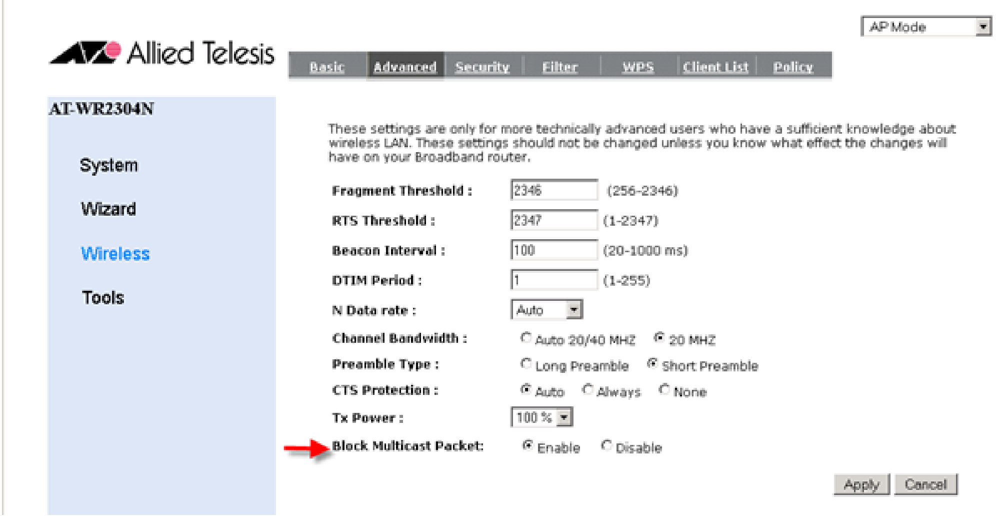
Bridge Type : Dynamic IP
802.1d Spanning Tree : Disabled

FIGURE 23-2 AT-WR2304N System Settings

8. Click **Apply**. You must click **Apply** on each page or changes will be lost.

By default, the wireless router floods multicast traffic to all LAN ports, including wireless.

9. To block multicast to wireless LAN ports, select the **Wireless** page, then select the **Advanced** tab.
10. For **Block Multicast Packet**, select **Enable**.



These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Broadband router.

Fragment Threshold : 2346 (256-2346)
RTS Threshold : 2347 (1-2347)
Beacon Interval : 100 (20-1000 ms)
DTIM Period : 1 (1-255)
N Data rate : Auto
Channel Bandwidth : ○ Auto 20/40 MHZ ● 20 MHZ
Preamble Type : ○ Long Preamble ● Short Preamble
CTS Protection : ● Auto ○ Always ○ None
Tx Power : 100 %
Block Multicast Packet: ● Enable ○ Disable

FIGURE 23-3 AT-WR2304N Wireless Settings

11. Click **Apply**.
12. Disconnect the computer from the wireless router.

23.5 Connecting the AT-WR2304N Wireless Router to the iMG

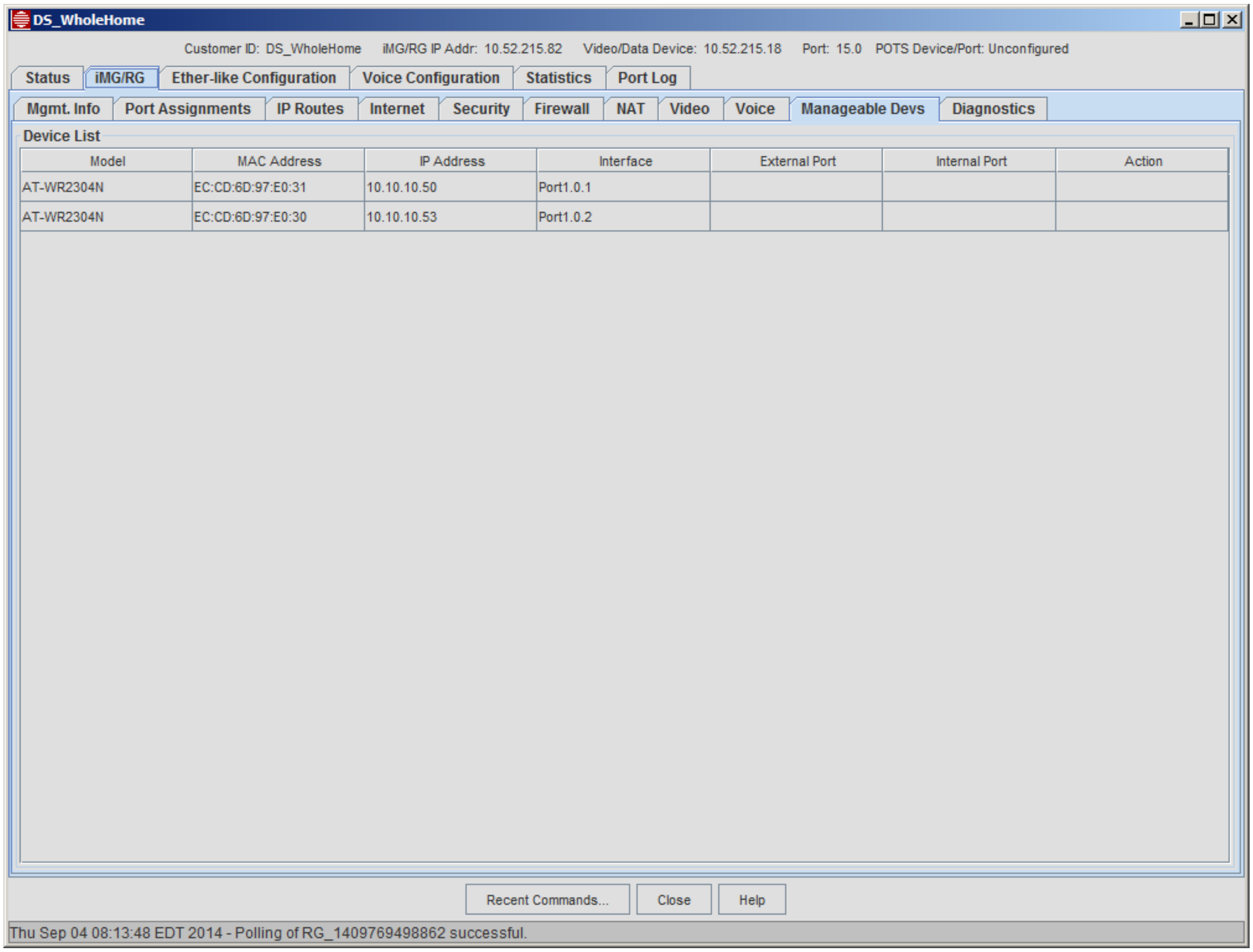
1. If it is not already powered on, power on the wireless router.

2. Connect a CAT5 cable from the AT-WR2304N WAN port to the iMG port you configured for Internet or Internet/ Video service.

To confirm the wireless router is connected correctly, see Browsing to the Wireless Router from the NMS.

23.6 Browsing to the Wireless Router from the NMS

1. Launch the NMS from a client machine.
2. In the **Network Objects** panel, go to **Network Inventory** > **iMG/RGs**.
3. In the **iMG/RGs** window, select the device with one or more wireless routers connected to the LAN interfaces.
4. Right-click, then select **View/Modify Details**. The device’s settings window appears.
5. Select the **iMG/RG** tab.
6. Select the Manageable Devs Tab. Available wireless routers are listed in the **Device List**.



Customer ID: DS_WholeHome iMG/RG IP Addr: 10.52.215.82 Video/Data Device: 10.52.215.18 Port: 15.0 POTS Device/Port: Unconfigured

Device List

Model	MAC Address	IP Address	Interface	External Port	Internal Port	Action
AT-WR2304N	EC:CD:6D:97:E0:31	10.10.10.50	Port1.0.1			
AT-WR2304N	EC:CD:6D:97:E0:30	10.10.10.53	Port1.0.2			

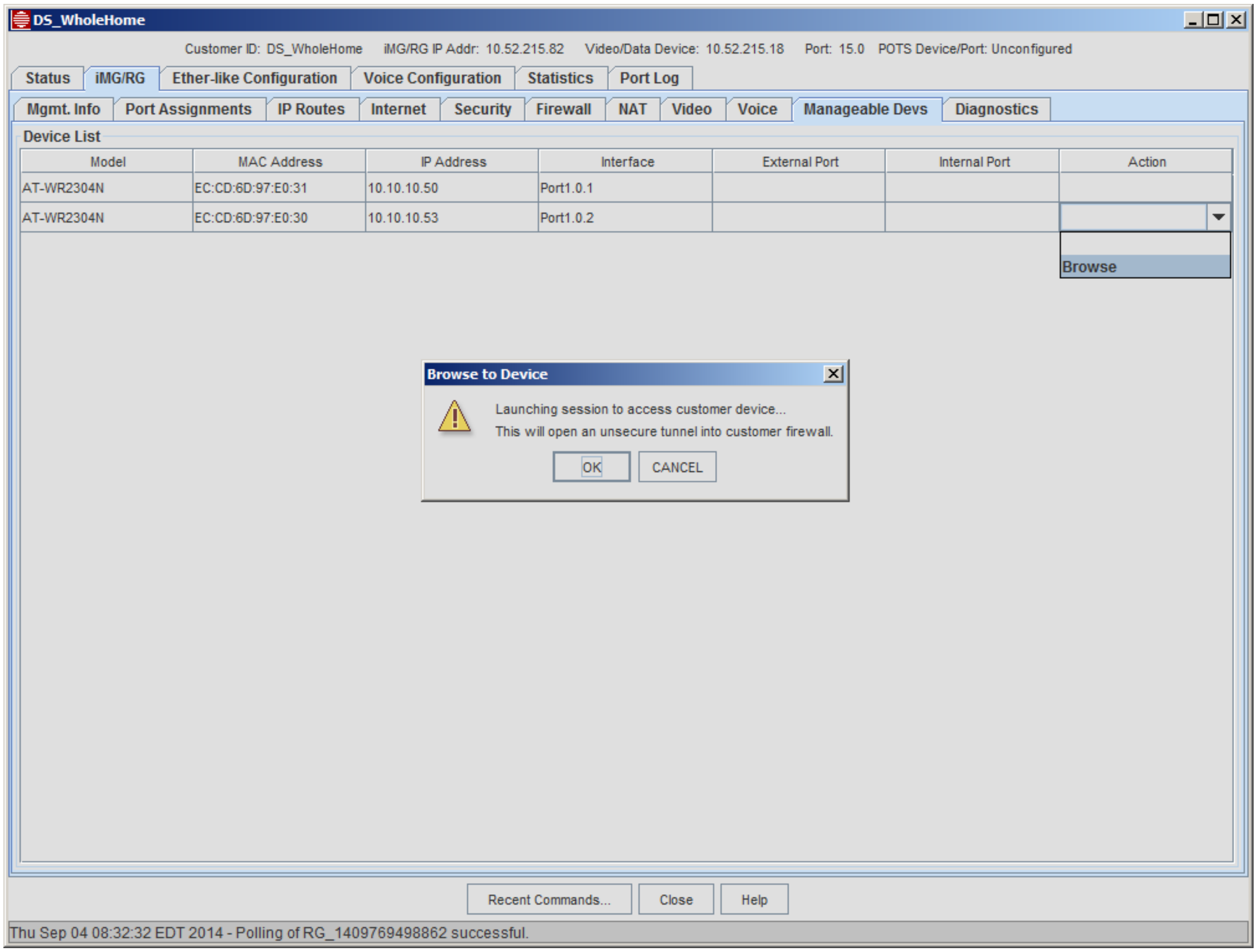
Thu Sep 04 08:13:48 EDT 2014 - Polling of RG_1409769498862 successful.

FIGURE 23-4 Manageable Devices Tab

7. Select the wireless router you want to manage.
8. If necessary, select the **External Port** field and enter a specific external port to use for this session. The default port is 5080.
9. If necessary, select the **Internal Port** field and enter a specific internal port to use for this session. The default port is 80.

Note: Port 80 must be used as the internal port with the AT-WR2304N in AP Mode.

10. In the **Action** drop-down list, select **Browse**. The **Browse to Device** dialog box appears.



Customer ID: DS_WholeHome iMG/RG IP Addr: 10.52.215.82 Video/Data Device: 10.52.215.18 Port: 15.0 POTS Device/Port: Unconfigured

Device List

Model	MAC Address	IP Address	Interface	External Port	Internal Port	Action
AT-WR2304N	EC:CD:6D:97:E0:31	10.10.10.50	Port1.0.1			
AT-WR2304N	EC:CD:6D:97:E0:30	10.10.10.53	Port1.0.2			

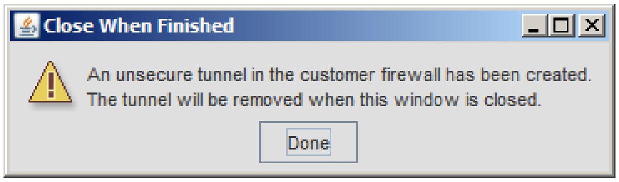
Launching session to access customer device...
This will open an unsecure tunnel into customer firewall.

Thu Sep 04 08:32:32 EDT 2014 - Polling of RG_1409769498862 successful.

FIGURE 23-5 Manageable Devs - Browse to Device

Note: *If you click Cancel in the Browse to Device dialog box, the external and internal port settings reset to their default values.*

11. Click **OK** to open an unsecure tunnel through the iMG and launch the wireless router's management web page. The **Close When Finished** dialog box appears.



An unsecure tunnel in the customer firewall has been created.
The tunnel will be removed when this window is closed.

FIGURE 23-6 Manageable Devs - Close When Finished

The wireless router's management page launches in the default browser. The URL is the IP address for the iMG's Internet VLAN interface. For example, http://10.52.110.69:5080.

Note: *The Close When Finished dialog box must remain open throughout the wireless router management session. If you close the dialog box, the connection to the wireless router will be lost.*

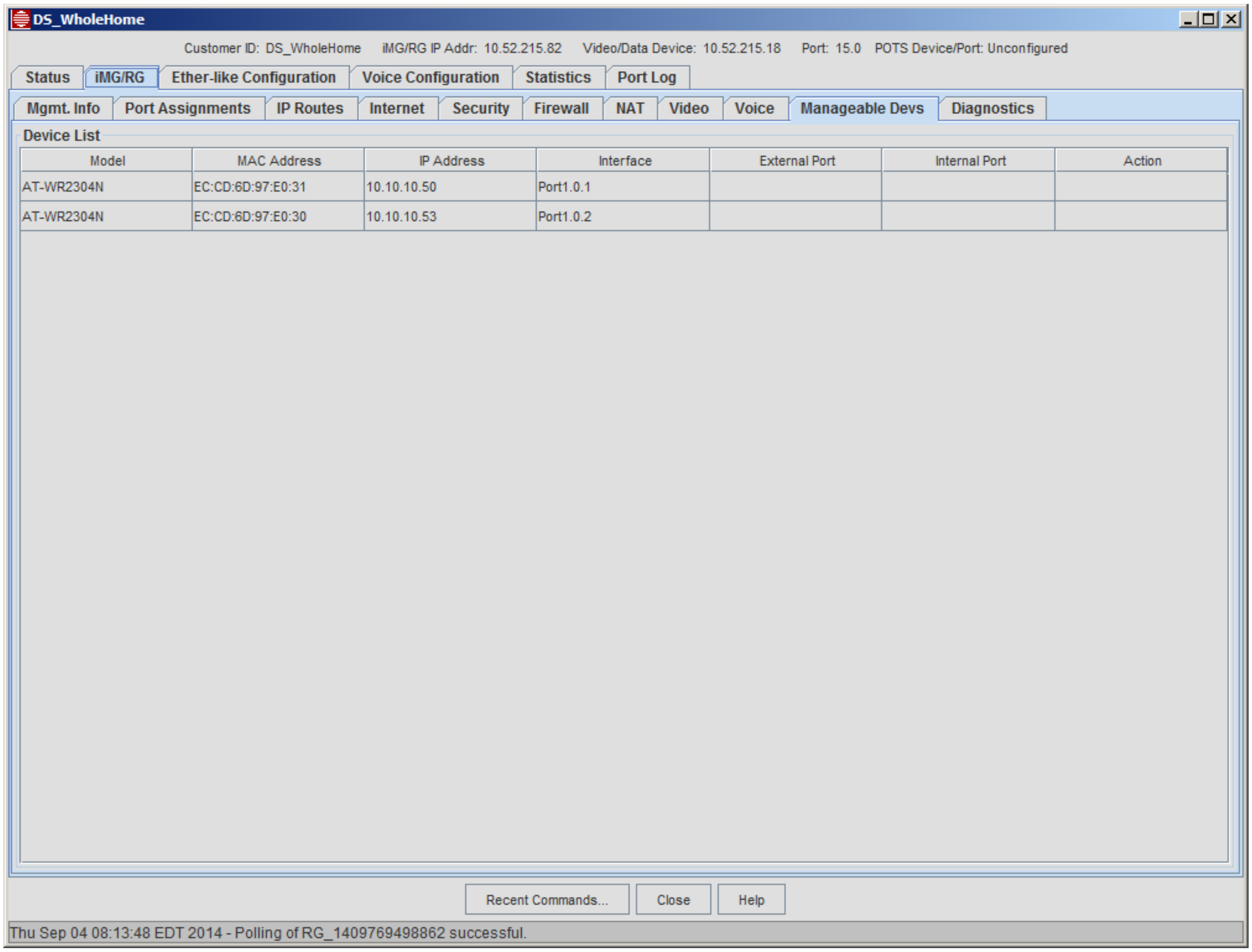
While the tunnel is open you cannot perform any other task in the NMS on the iMG screen.

12. Log into the device. The default username and password are:

username: manager
password: friend

13. When you are finished managing the wireless router, in the **Close When Finished** dialog box, click **Done**. The NMS closes the connection to the wireless router and removes the tunnel from the iMG.

23.6.1 Manageable Devs Tab



Customer ID: DS_WholeHome iMG/RG IP Addr: 10.52.215.82 Video/Data Device: 10.52.215.18 Port: 15.0 POTS Device/Port: Unconfigured

Model	MAC Address	IP Address	Interface	External Port	Internal Port	Action
AT-WR2304N	EC:CD:6D:97:E0:31	10.10.10.50	Port1.0.1			
AT-WR2304N	EC:CD:6D:97:E0:30	10.10.10.53	Port1.0.2			

Thu Sep 04 08:13:48 EDT 2014 - Polling of RG_1409769498862 successful.

TABLE 23-3 Manageable Devs Tab

Column	Description
Model	The wireless router model number.
MAC Address	The MAC address of the wireless router.
IP Address	The IP address for the wireless router.
Interface	The iMG port the wireless router is subtended off of.
External Port	The WAN TCP port the iMG uses to listen for incoming requests. Connections made to this port from the public network to the iMG are forwarded to the wireless router. The default is 5080 for the first external port. The port number increments by one for each additional device.

TABLE 23-3 Manageable Devs Tab (Continued)

Column	Description
Internal Port	The WAN TCP port the wireless router uses to listen for incoming connections. The default is 80.
Action	The action to take to connect with the wireless router. Browse - Open the device’s management web page in a browser.

24. Triple Play Examples

Before you fill out the Triple-Play form make sure you perform the following:

- Create the relevant iMG profiles.
- Create the relevant iMAP port profiles.
- If voice service is being provided, configure the initial voice handling (such as G6).

Refer to Provision a New Triple Play Customer for an overview of the Triple Play form and its fields. Once the profiles have been defined, they are included in datafilling the triple play form. The form includes a pull-down where the administrator chooses which RG General profile will be applied to the RG that interfaces the iMAP port. The fields that appear depend on the RG General Profile chosen and the services that are going to be configured on the RG.

The Provision New Triple Play Customer Form is used to provision on one form most of the attributes needed for one Triple Play customer. The fields of the Provision New Triple Play Customer Form are described in Provision a New Triple Play Customer.

The form is divided into four main panels: RG, Video/Data Configuration, Video/Data Configuration and Derived Voice.

Using this form is an efficient and error-free method to data fill a customer, and this becomes even more true when used in conjunction with Profiles and the use of Scoping. Following are examples:

1. An iMG624A with the following services and components: (Configuration 1 Example - POTS, Derived Voice, Internet, Video, TLS)

- A PC with internet service
- Two video LAN ports for video service (two STBs)
- A Transparent LAN Service (TLS that provides a secure and isolated VLAN for customers (802.3).
- Two levels of phone service

  - POTS24 based phone

  - Derived phone service

2. An RG646 with the following services and components: (Configuration 2 - Multiple Video, Data, Derived Voice)

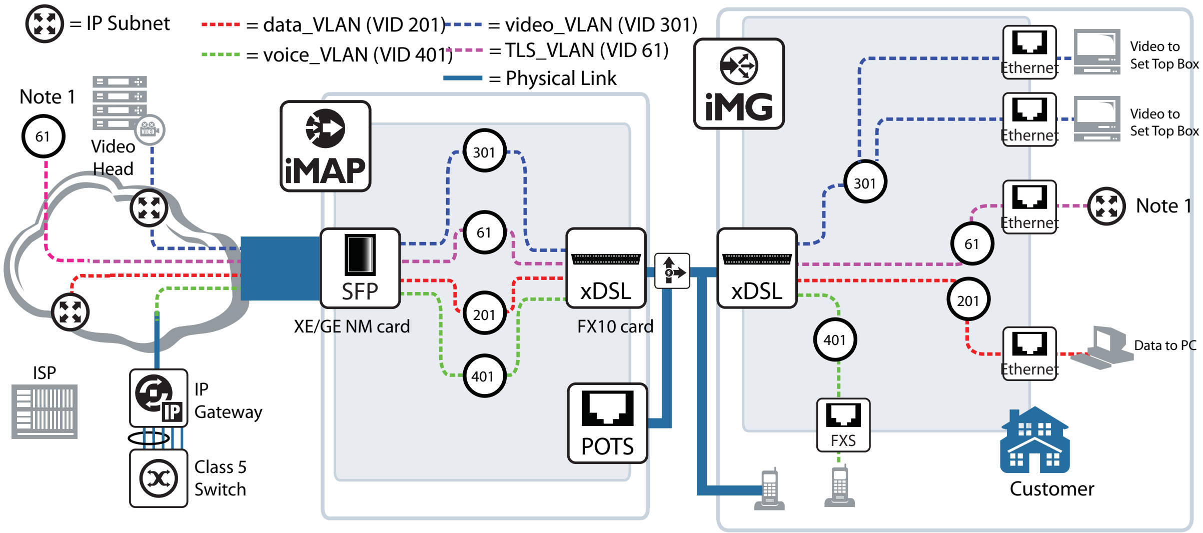
- Five videos for video service (five STBs)
- A pc with internet service
- A phone that is provisioned but not configured, so it can be easily done later.

3. A statically configured RG, usually for demonstration only. (Configuration 3 - Static Provisioning (no DHCP))
4. An EPON/ONU interface connected with the iMG646PX-ON. (Configuration 4 - EPON/ONU Interface Connected with iMG646PX-ON)
5. An RG634 similar to example 1, but with SIP being used for Voice Service. (Configuration 5 - Voice Service Provided by SIP)
6. A multi-service VLAN (more than one service on one VLAN). (Configuration 6 - Multi-Service VLAN)
7. An iMG6x6MOD configuration (Configuration 7 - iMG7x6MOD with HPNA)
8. An AlliedWare Plus Device (Configuration 8 - AlliedWare Plus Device)
9. Microsoft© Mediaroom™ with the iMG/RG (Configuration 9 - Microsoft Mediaroom with the iMG/RG)

10. Video with static IP Address (Configuration 10 - Video with static IP Address (iMG 1000 and iMG 2000 Series))

Following each figure is the **Provision New Triple Play Customer Form** filled out for each configuration.

24.1 Configuration 1 Example - POTS, Derived Voice, Internet, Video, TLS



Note 1Connects to separate business network

FIGURE 24-1 Example Configuration 1 - Internet Routed/NAT, Video Proxy, Lifeline POTS, TLS

TABLE 24-1 Example Profiles for Configuration 1 - with RG 624

Profile Type	Example Profile Name	Description
Upstream Port Profile	“Auto2+ w/NoFA”	Profile name provides description: Auto2+ = ADSL mode used w/NoFA = with No Filtering and No Ageing
RG General Profile	“DVLKND-AI01-P-1I_2V_1T”	Profile name provides description: DVLKND-AI01- = Access Island 01 P = Phone (Derived Voice) 1I = 1 internet 2V = 2 Video 1T = 1 TLS
RG Internet Profile	“Bridged Int Srv”	
RG Video Profile	“Video-Flood”	A way to highlight the NONE type service, since with no snooping there is flood forwarding. Since there are less than three STBs, this is supported.

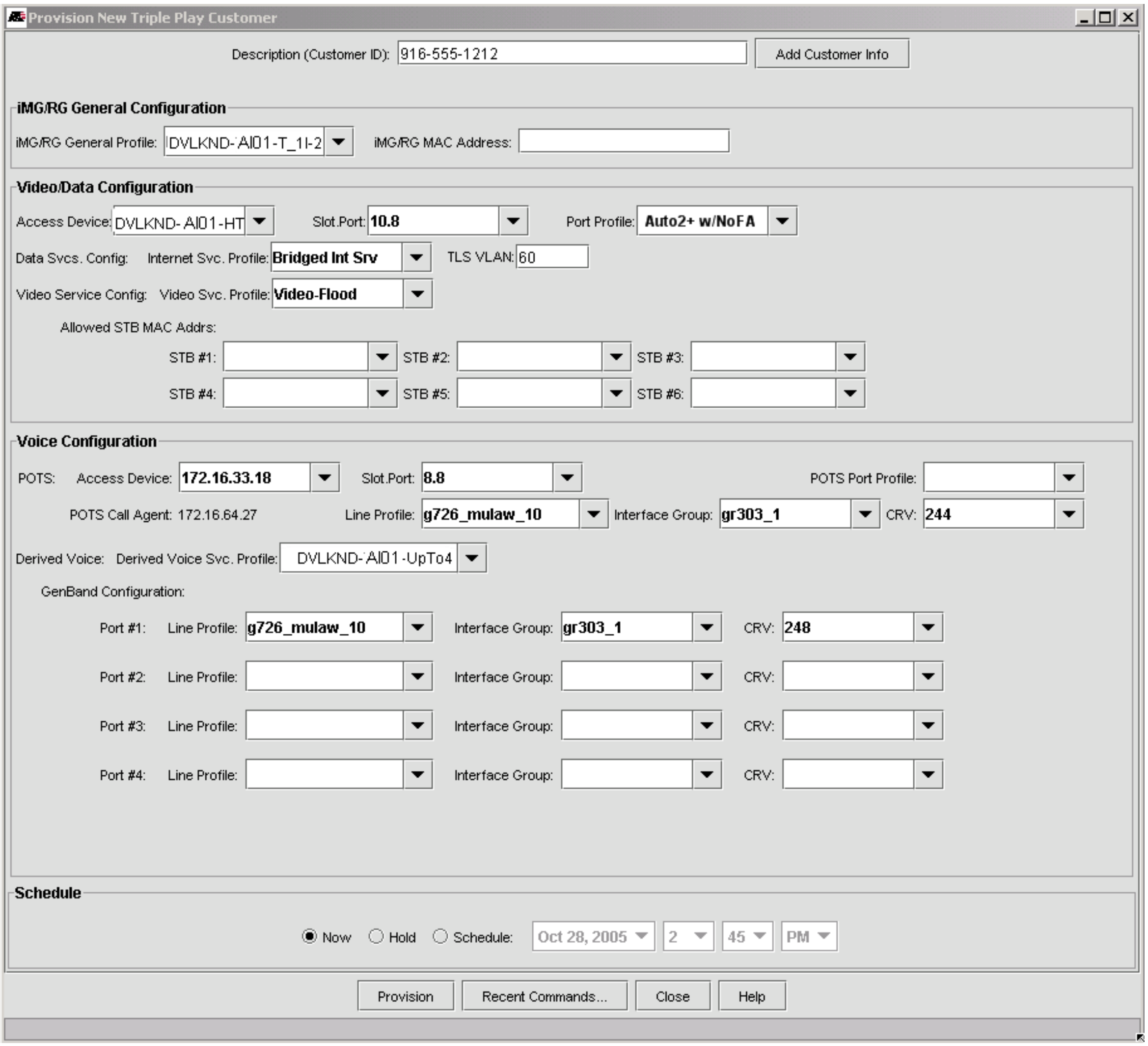
TABLE 24-1 Example Profiles for Configuration 1 - with RG 624

Profile Type	Example Profile Name	Description
RG Voice Profile	“DVLKND-AI01-UpTo4Line”	This is generic for derived voice for Access Island 01; with this profile there is no risk of deprovisioning a derived voice line Using the battery is not reflected in the Profile
Line Profile	g726_mulaw_10	Provides specific attributes for G6 voice channel for POTS and Derived Voice. (These were part of the initial G6 setup.) This field determines the Interface Groups available which in term determines the CRVs available. These values are usually part of a work order

The following figure shows how the Triple Play form is filled out to reflect these profiles, since most of the values are automatically datafilled when the Profiles are included.

Note the use of Scoping for both the RG General and the RG Voice Profiles, as shown in Figure 24-3 and Figure 24-4. The Profile Scoping field is set to the Access Island Prefix (AI01) with the wildcard (*). When the user brings up the Triple Play form and chooses a device, the available General and Voice profiles are based on the scope set. Conversely, if the user chooses a General or Derived Voice Profile with the scope set, only Access Devices that are within that scope are available.

Note: If the user is deploying (or re-deploying) an RG General Profile that includes TLS to an RG that has not been configured for TLS, there will be a prompt for the user to enter the TLS VLAN, which must be previously created.



Provision New Triple Play Customer

Description (Customer ID): 916-555-1212 [Add Customer Info]

iMG/RG General Configuration

iMG/RG General Profile: DVLKND-AI01-T_1I-2 iMG/RG MAC Address:

Video/Data Configuration

Access Device: DVLKND-AI01-HT Slot.Port: 10.8 Port Profile: Auto2+ w/NoFA

Data Svcs. Config: Internet Svc. Profile: Bridged Int Srv TLS VLAN: 60

Video Service Config: Video Svc. Profile: Video-Flood

Allowed STB MAC Addrs:

STB #1: STB #2: STB #3:

STB #4: STB #5: STB #6:

Voice Configuration

POTS: Access Device: 172.16.33.18 Slot.Port: 8.8 POTS Port Profile:

POTS Call Agent: 172.16.64.27 Line Profile: g726_mulaw_10 Interface Group: gr303_1 CRV: 244

Derived Voice: Derived Voice Svc. Profile: DVLKND-AI01-UpTo4

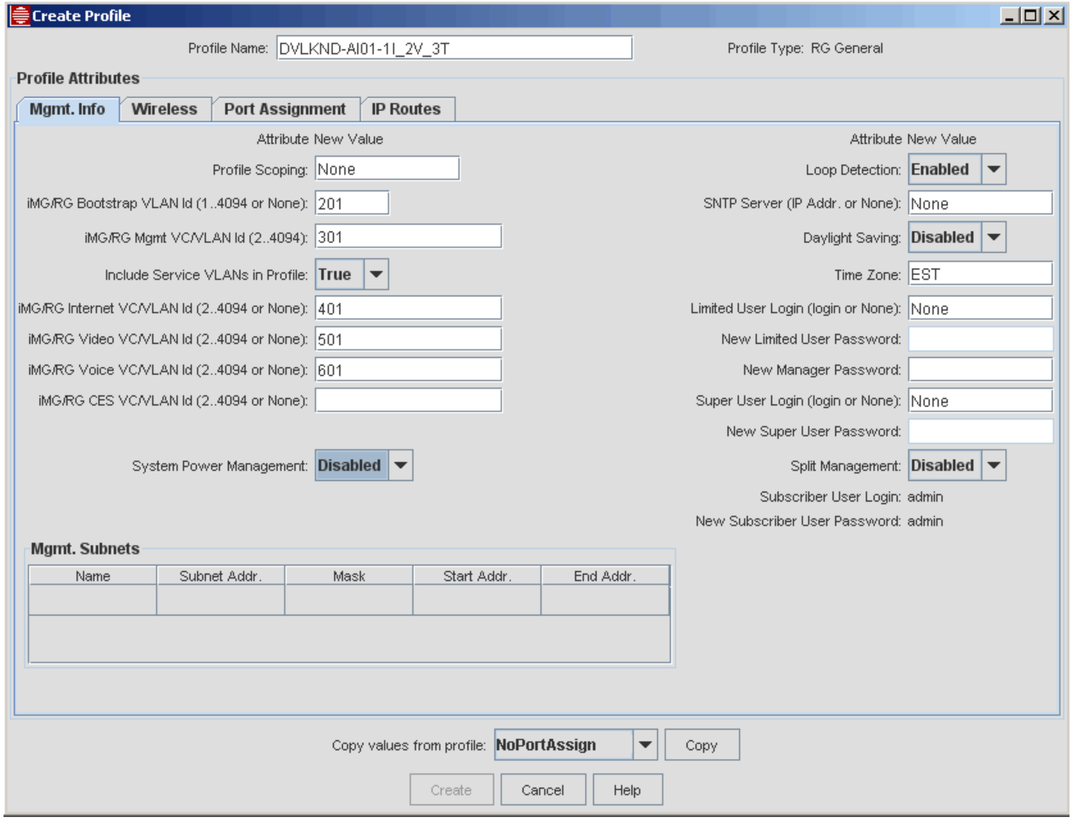
GenBand Configuration:

Port #1:	Line Profile: g726_mulaw_10	Interface Group: gr303_1	CRV: 248
Port #2:	Line Profile:	Interface Group:	CRV:
Port #3:	Line Profile:	Interface Group:	CRV:
Port #4:	Line Profile:	Interface Group:	CRV:

Schedule

● Now ○ Hold ○ Schedule: Oct 28, 2005 2 45 PM

FIGURE 24-2 Triple Play Customer Form for RG 634 - Two Voice, Two Video, TLS, and One Internet



Profile Name: DVLKND-AI01-1I_2V_3T

Profile Type: RG General

Profile Attributes

Attribute New Value

Profile Scoping: None

iMG/RG Bootstrap VLAN Id (1..4094 or None): 201

iMG/RG Mgmt VC/VLAN Id (2..4094): 301

Include Service VLANs in Profile: True

iMG/RG Internet VC/VLAN Id (2..4094 or None): 401

iMG/RG Video VC/VLAN Id (2..4094 or None): 501

iMG/RG Voice VC/VLAN Id (2..4094 or None): 601

iMG/RG CES VC/VLAN Id (2..4094 or None):

System Power Management: Disabled

Attribute New Value

Loop Detection: Enabled

SNTP Server (IP Addr. or None): None

Daylight Saving: Disabled

Time Zone: EST

Limited User Login (login or None): None

New Limited User Password:

New Manager Password:

Super User Login (login or None): None

New Super User Password:

Split Management: Disabled

Subscriber User Login: admin

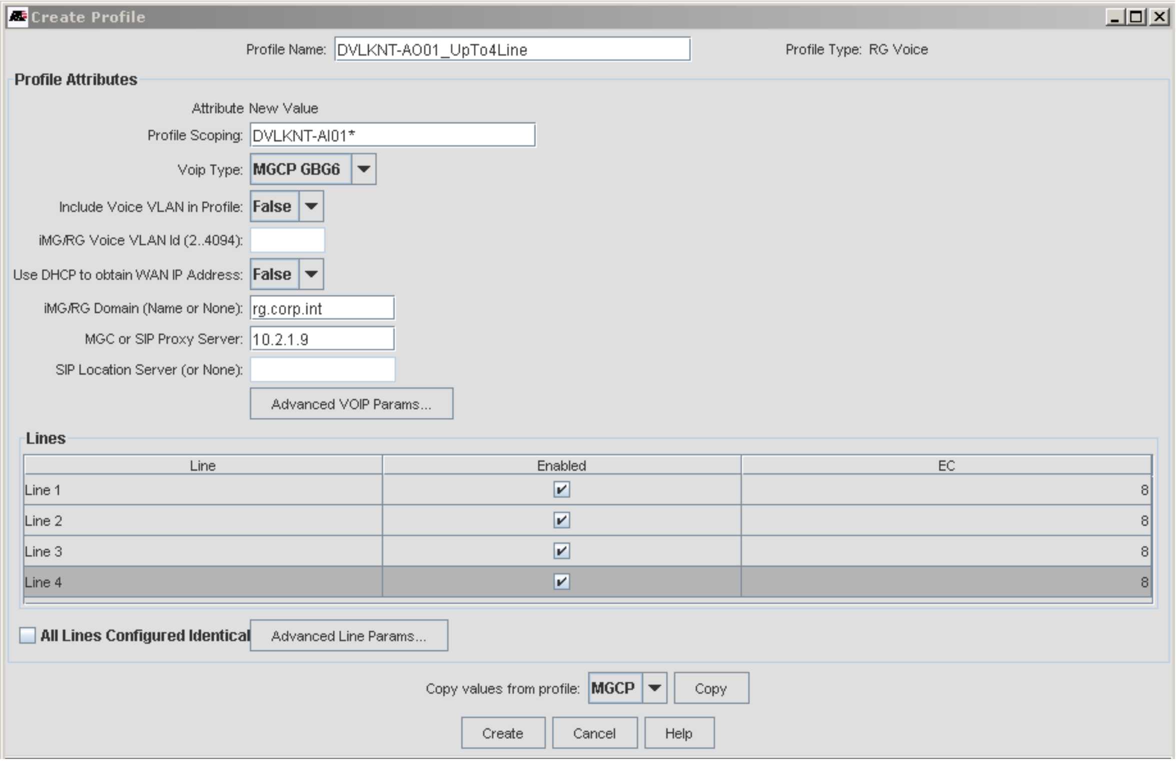
New Subscriber User Password: admin

Mgmt. Subnets

Name	Subnet Addr.	Mask	Start Addr.	End Addr.

Copy values from profile: NoPortAssign

FIGURE 24-3 RG General Profile for Configuration 1



Profile Name: DVLKNT-AO01_UpTo4Line

Profile Type: RG Voice

Profile Attributes

Attribute New Value

Profile Scoping: DVLKNT-AI01*

Voip Type: MGCP GBG6

Include Voice VLAN in Profile: False

iMG/RG Voice VLAN Id (2..4094):

Use DHCP to obtain WAN IP Address: False

iMG/RG Domain (Name or None): rg.corp.int

MGC or SIP Proxy Server: 10.2.1.9

SIP Location Server (or None):

Lines

Line	Enabled	EC
Line 1	☑	8
Line 2	☑	8
Line 3	☑	8
Line 4	☑	8

□ All Lines Configured Identical

Copy values from profile: MGCP

FIGURE 24-4 RG Voice Profile for Configuration 1

24.2 Configuration 2 - Multiple Video, Data, Derived Voice

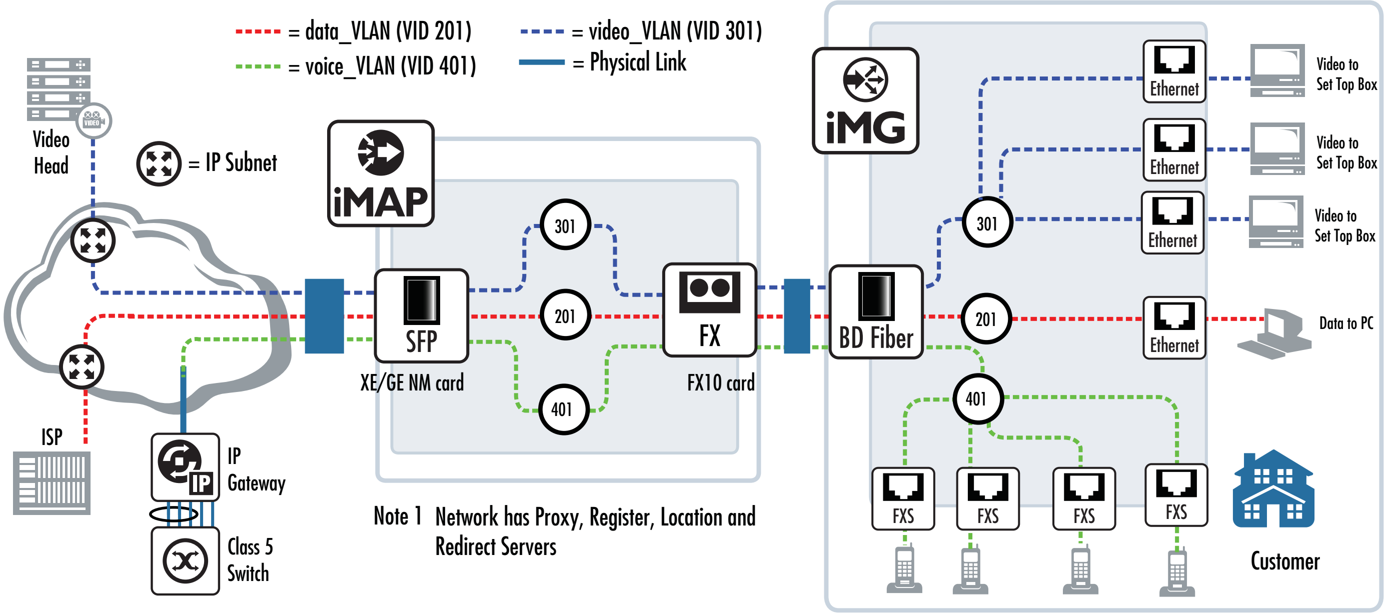


FIGURE 24-5 Configuration 2 - Three Video and One Internet Connection

In this configuration, there are three video devices and one PC with a bridged service. The iMAP customer interface supports up to eight DHCP Auto-filters. With the three STBs and one PC, this is easily supported, although for any changes the administrator should consider the following:

- There should be no “nesting” of STBs behind a local switch.
- If more than one port is used for internet service, using internet NAT service should be considered since the iMAP would only see one DHCP object.

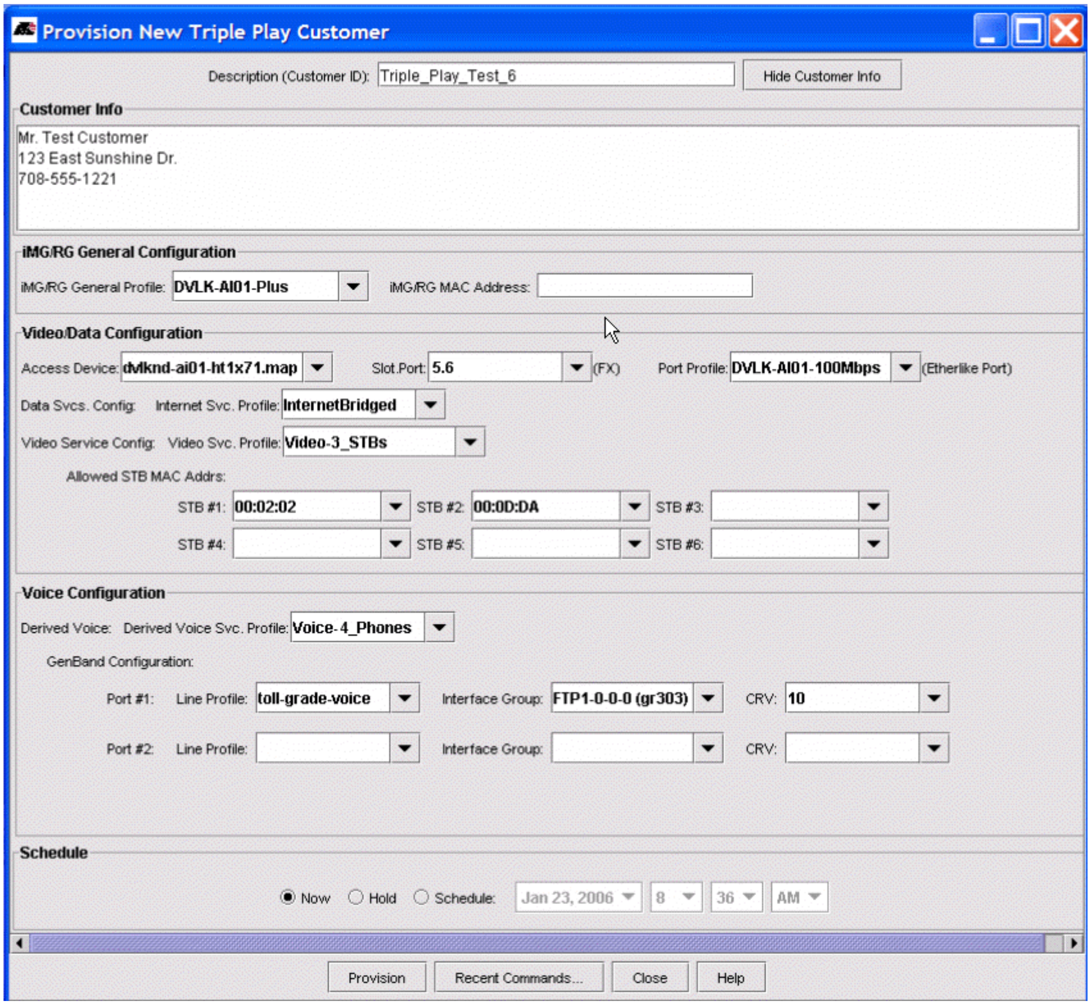
Finally, if more than one port is used for internet service, each port should have a rate limiting rate set in the Profile to prevent possible blocking/pixel loss for the video service ports.

TABLE 24-2 Example Profiles for Configuration 2

Profile Type	Example Profile Name	Description
Upstream Port Profile	“100Mbps”	Stands for Ethernet to the Customer Premises with no Filtering and No Ageing, on an Ethernet 100Mbps.
RG General Profile	“DVLKND-AI01-Plus”	Stands for Access Island AI01
RG Internet Profile	“InternetBridged”	Stands for Routed NAT service with the firewall enabled
RG Video Profile	“Video-3_STBs_SNOOP”	With three STBs, snooping will help with controlling bandwidth to each STB
RG Voice Profile	“Voice-4_Phones”	Generic, to always allow up to four derived voice

The following figure shows how the Triple Play form is filled out to reflect these profiles, since most of the values are automatically datafilled when the Profiles are included.

Note the use of Scoping for both the RG General and the RG Voice Profiles, as shown in Figure 24-7. The Profile Scoping field is set to the Access Island Prefix (AI01) with the wildcard (*). When the user brings up the Triple Play form and chooses a device, the available General and Voice profiles are based on the scope set.



Description (Customer ID): Triple_Play_Test_6

Customer Info

Mr. Test Customer
123 East Sunshine Dr.
708-555-1221

iMG/RG General Configuration

iMG/RG General Profile: DVLK-AI01-Plus iMG/RG MAC Address:

Video/Data Configuration

Access Device: dvlknd-ai01-ht1x71.map Slot.Port: 5.6 (FX) Port Profile: DVLK-AI01-100Mbps (Etherlike Port)

Data Svcs. Config: Internet Svc. Profile: InternetBridged

Video Service Config: Video Svc. Profile: Video-3_STBs

Allowed STB MAC Addrs:

STB #1: 00:02:02 STB #2: 00:0D:DA STB #3:

STB #4: STB #5: STB #6:

Voice Configuration

Derived Voice: Derived Voice Svc. Profile: Voice-4_Phones

GenBand Configuration:

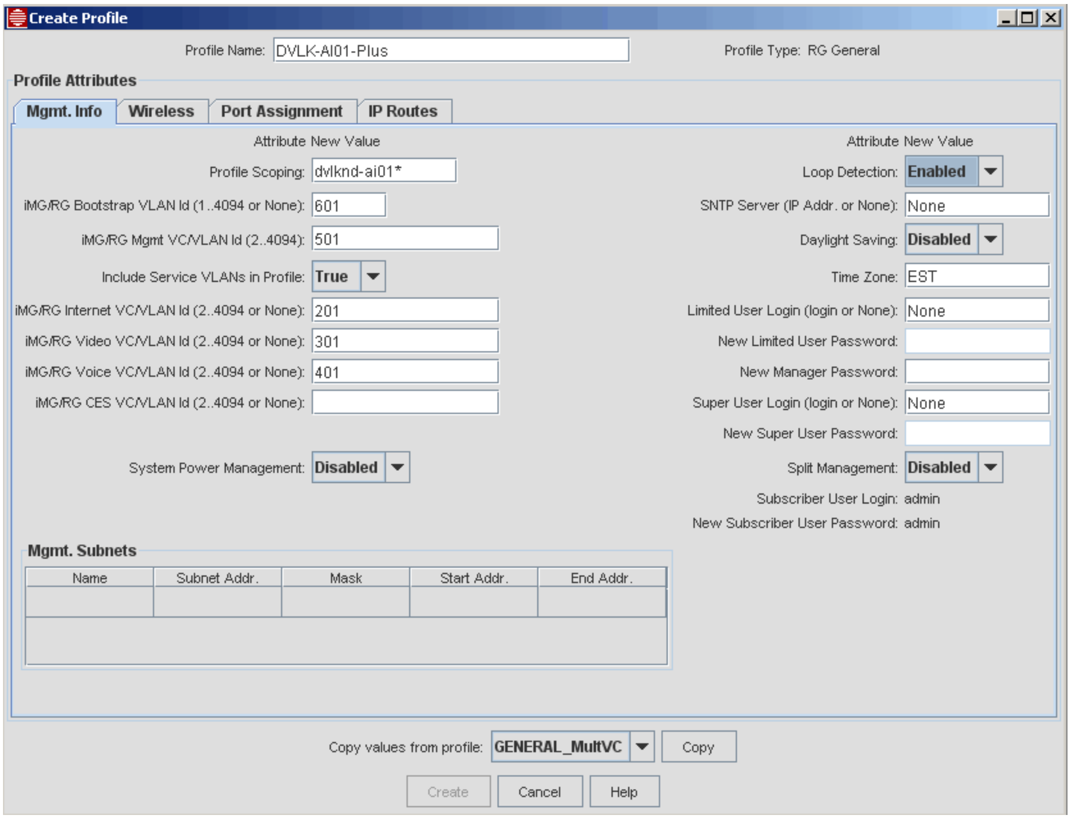
Port #1: Line Profile: toll-grade-voice Interface Group: FTP1-0-0-0 (gr303) CRV: 10

Port #2: Line Profile: Interface Group: CRV:

Schedule

● Now ○ Hold ○ Schedule: Jan 23, 2006 8 36 AM

FIGURE 24-6 Triple Play Customer Form for RG 646 - Configuration 2



Profile Name: DVLK-AI01-Plus

Profile Type: RG General

Profile Scoping: dvlknd-ai01*

iMG/RG Bootstrap VLAN Id (1..4094 or None): 601

iMG/RG Mgmt VC/VLAN Id (2..4094): 501

Include Service VLANs in Profile: True

iMG/RG Internet VC/VLAN Id (2..4094 or None): 201

iMG/RG Video VC/VLAN Id (2..4094 or None): 301

iMG/RG Voice VC/VLAN Id (2..4094 or None): 401

iMG/RG CES VC/VLAN Id (2..4094 or None):

System Power Management: Disabled

Loop Detection: Enabled

SNTP Server (IP Addr. or None): None

Daylight Saving: Disabled

Time Zone: EST

Limited User Login (login or None): None

New Limited User Password:

New Manager Password:

Super User Login (login or None): None

New Super User Password:

Split Management: Disabled

Subscriber User Login: admin

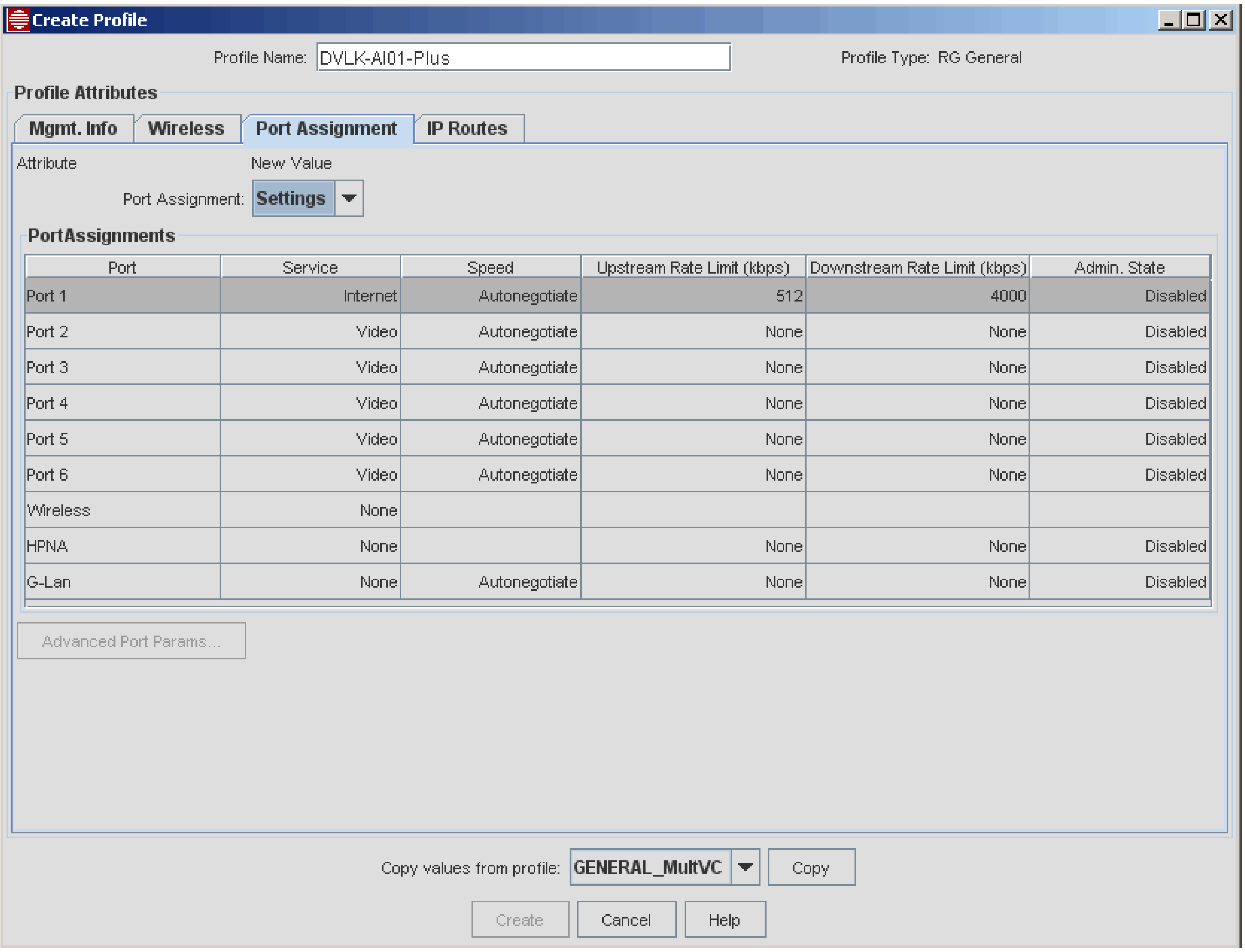
New Subscriber User Password: admin

Mgmt. Subnets

Name	Subnet Addr.	Mask	Start Addr.	End Addr.

Copy values from profile: GENERAL_MultVC

FIGURE 24-7 RG General Profile for Configuration 2 - Mgmt. Info



Profile Name: DVLK-AI01-Plus

Profile Type: RG General

Port Assignment: Settings

PortAssignments

Port	Service	Speed	Upstream Rate Limit (kbps)	Downstream Rate Limit (kbps)	Admin. State
Port 1	Internet	Autonegotiate	512	4000	Disabled
Port 2	Video	Autonegotiate	None	None	Disabled
Port 3	Video	Autonegotiate	None	None	Disabled
Port 4	Video	Autonegotiate	None	None	Disabled
Port 5	Video	Autonegotiate	None	None	Disabled
Port 6	Video	Autonegotiate	None	None	Disabled
Wireless	None				
HPNA	None		None	None	Disabled
G-Lan	None	Autonegotiate	None	None	Disabled

Copy values from profile: GENERAL_MultVC

FIGURE 24-8 RG General Profile for Configuration 2 - Port Assignment

Once the RG is pre-provisioned, it appears in the Network Inventory View under iMG/RGs. Right clicking on the device and selecting View/Modify Details brings up the tabbed form that includes all of the device attributes. Provisioning the iMG Managed Object Properties goes through these tabs and highlights important attributes.

Note: Refer to Overview of Triple Play Service Management Form for an overview of the Triple Play Service Management Form and how it can be used to change the configuration.

24.3 Configuration 3 - Static Provisioning (no DHCP)

For a quick demonstration, an RG can be configured (providing all services and management addresses) using static provisioning; once some profiles are set up, hard-coded values are filled in for the forms.

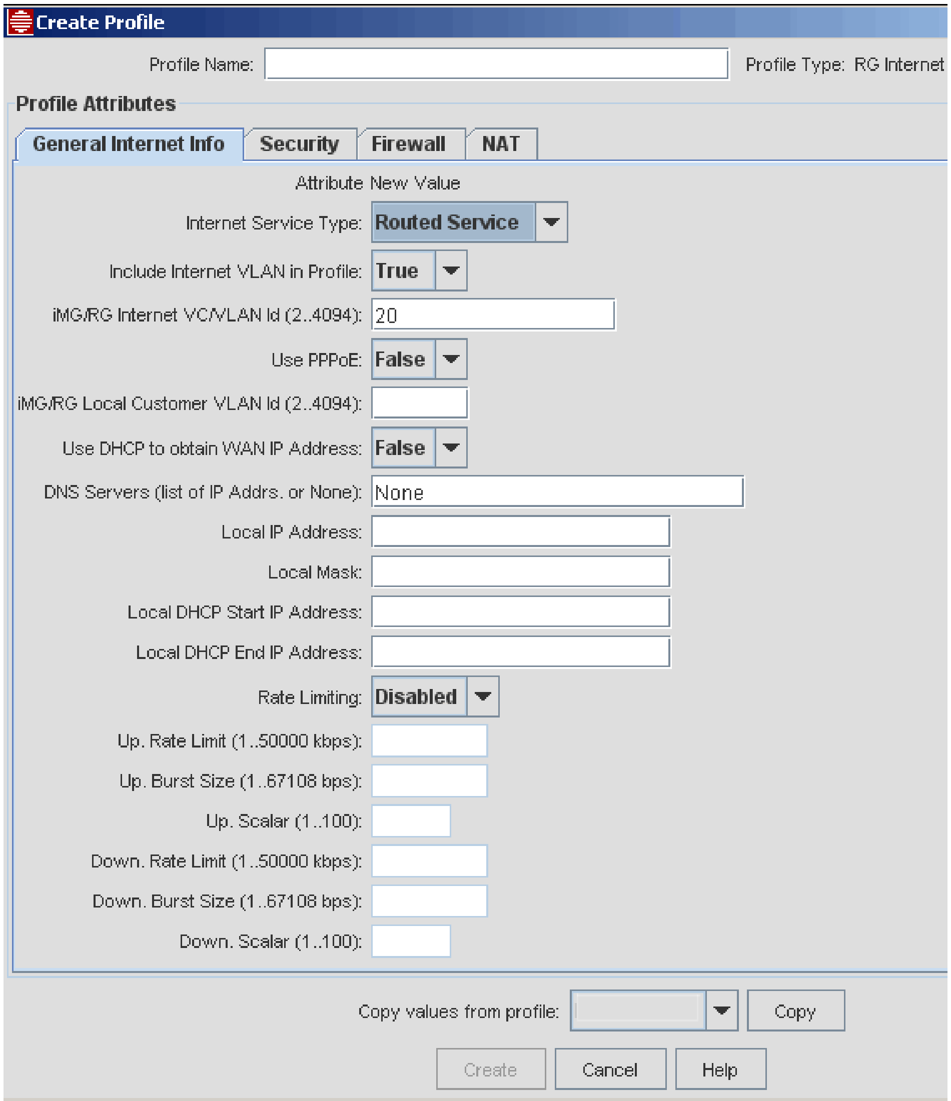
24.3.1 Prerequisites (Profiles and Hard-coded Values)

Before setting up a static model, the user should create some profiles that in critical ways do not have certain values filled in. This will control the Triple Play form when these Profiles are chosen.

The following figures show two profiles:

- HomeNetworkInet-StaticIP - Note that the Use DHCP to Obtain IP Address is set to False.

- VOIPPhone - StaticIP - Note that the Use DHCP to Obtain IP Address is set to False and the iMG/RG Domain is set to None.



Profile Name:

Profile Type: RG Internet

Attribute New Value

Internet Service Type: Routed Service

Include Internet VLAN in Profile: True

iMG/RG Internet VC/VLAN Id (2..4094): 20

Use PPPoE: False

iMG/RG Local Customer VLAN Id (2..4094):

Use DHCP to obtain WAN IP Address: False

DNS Servers (list of IP Addrs. or None): None

Local IP Address:

Local Mask:

Local DHCP Start IP Address:

Local DHCP End IP Address:

Rate Limiting: Disabled

Up. Rate Limit (1..50000 kbps):

Up. Burst Size (1..67108 bps):

Up. Scalar (1..100):

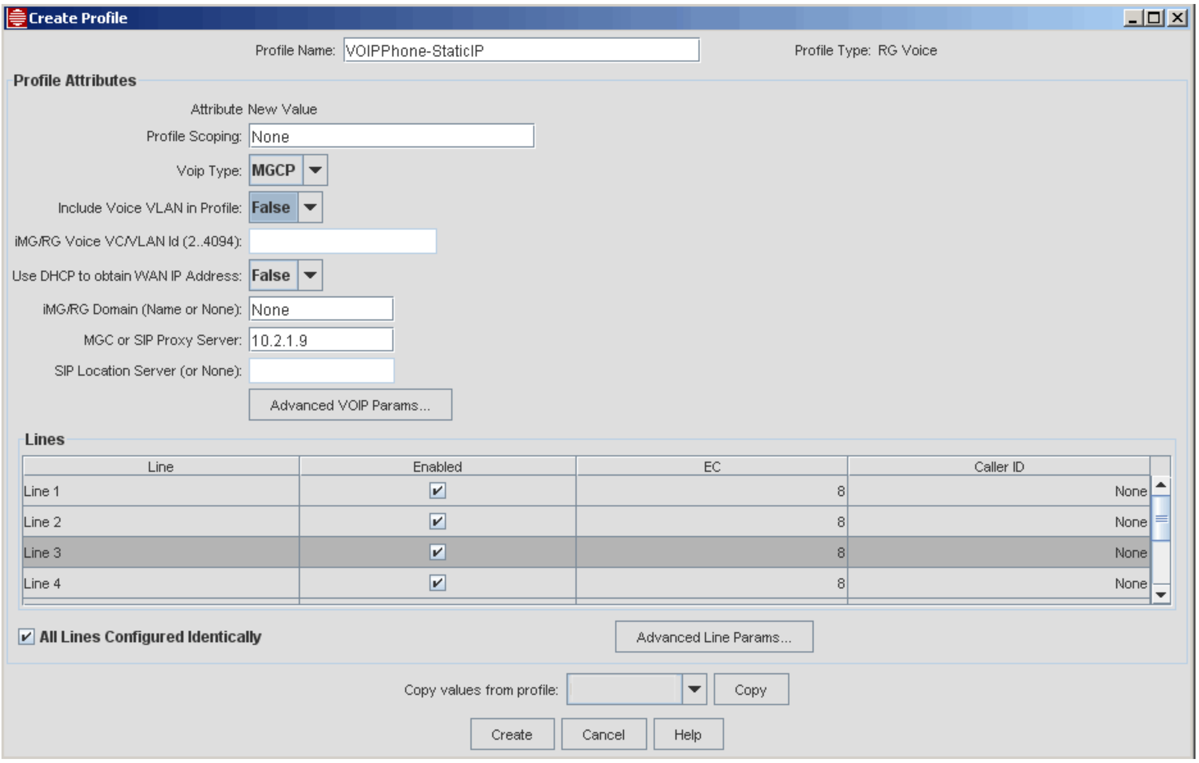
Down. Rate Limit (1..50000 kbps):

Down. Burst Size (1..67108 bps):

Down. Scalar (1..100):

Copy values from profile:

FIGURE 24-9 Internet Profile - no DHCP



Create Profile

Profile Name: VOIPPhone-StaticIP

Profile Type: RG Voice

Profile Attributes

Attribute New Value

Profile Scoping: None

Voip Type: MGCP

Include Voice VLAN in Profile: False

iMG/RG Voice VC/VLAN Id (2..4094):

Use DHCP to obtain WAN IP Address: False

iMG/RG Domain (Name or None): None

MGC or SIP Proxy Server: 10.2.1.9

SIP Location Server (or None):

Lines

Line	Enabled	EC	Caller ID
Line 1	☑	8	None
Line 2	☑	8	None
Line 3	☑	8	None
Line 4	☑	8	None

☑ All Lines Configured Identically

Copy values from profile:

FIGURE 24-10 RG Voice Profile - Static Configuration

Moreover, some hard-coded values must be known before beginning the procedure, since these static Profiles will make certain fields appear that must be filled in on the Triple Play form:

- RGMgmt IP Address - This does not need to be known if the user sets up discovery so that the IP address is included in the Discovery process. In most cases, however, the user must have a unique IP address and will associate this with the RGMgmt VLAN. This is highlighted in the next subsection.
- Internet service IP Address
- Voice Service IP Address
- Masks for the IP Addresses
- MAC address for the iMG/RG

24.3.2 Setting Up the IP Address for the iMG/RG

To give the iMG/RG a manual IP address, and to associate this address with the RGMgmt VLAN, the user should perform the following, noting that the procedure is different for Ethernet vs. ADSL types.

1. Choose the method of giving the iMG./RG the unique IP address depending on the type.

- For Ethernet:
  1. Connect an iMG/RG ethernet console port to the console port of a PC.

Note: The console cable is sold separately by ATI. Use n-8-1-38400 for the console port setting.

  2. Log in to the iMG/RG and set up the unique IP address

- For ADSL
  1. Connect the PC ethernet port to a LAN port on an iMG/RG.
  2. Power cycle the ADSL modem.

3. While the modem is powering up/reconnecting, hold the reset button of the RG for ~30 seconds.
4. The ADSL modem now has the following:

- IP Interface of ip0

- VLAN=1 untagged

- IP address = 192.168.1.1

- DHCP=Off

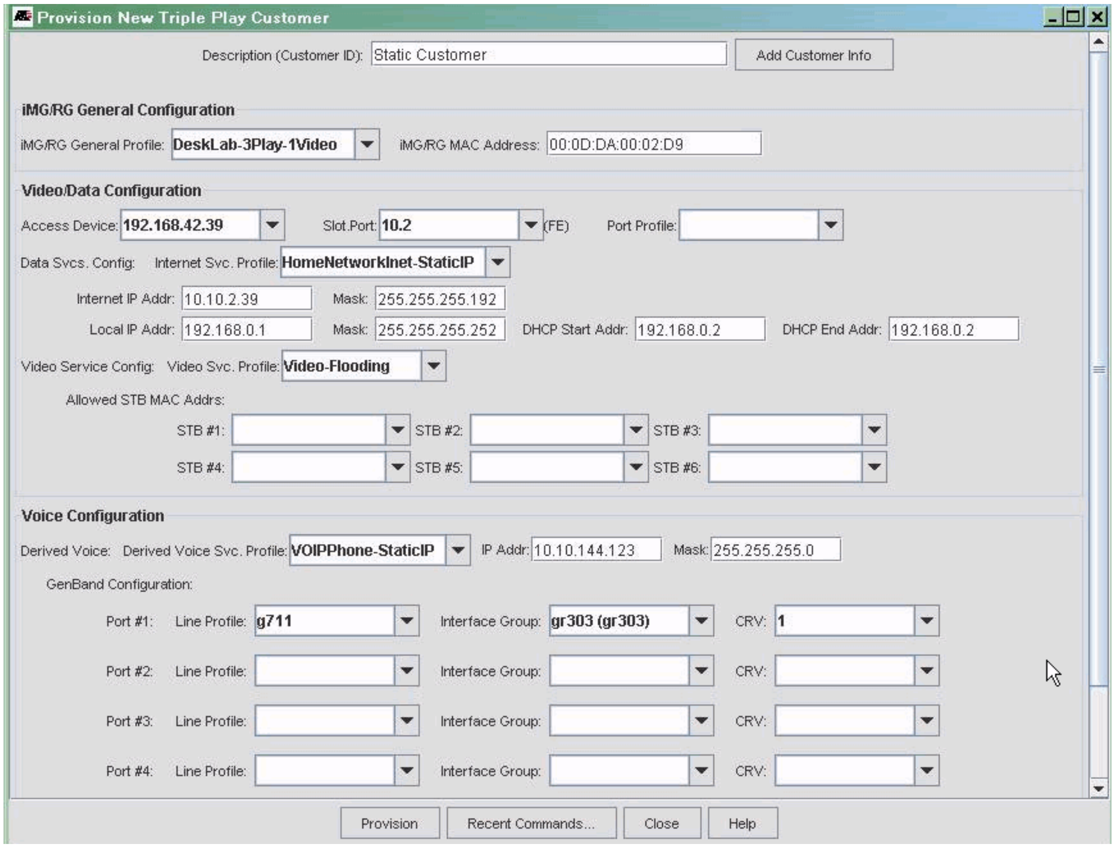
5. telnet into the ADSL modem using the 192.168.1.1 address.
6. Change the IP address to the unique IP address.
7. Save the configuration and set this as the default - You can now take the RG to the customer site if not already there.

24.3.3 Filling out the Triple-Play Form

Using the Profiles described above and the hard-coded values, the user can fill out the Triple-Play form, as shown in the following figure. Key fields are in the table below.

TABLE 24-3 Triple-Play Form Values for Example Static Configuration

Field	Value	Notes
Description	Static Customer	Since this is usually a for demonstration, should describe type of configuration
iMG/RG MAC Address	00:0D:DA:00:02:D9	
Access Device Name Slot.Port	192.168.42.39 10.2	Not required if the iMG/RG is not connected to the iMAP.
Internet Svc. Profile	HomeNetworkInet-StaticIP	Refer to Prerequisites (Profiles and Hard-coded Values). When this profile is entered, values that are normally created by DHCP are now editable.
Internet IP Addr Mask	10.10.2.39 255.255.255.192	Internet Subnet
Local IP Addr. Mask	192.168.0.1 255.255.255.252	IP address for the RG
DHCP Start Addr. DHCP End Addr.	192.168.0.2 192.168.0.2	for customer side addresses when RG acts as DHCP server
Derived Voice Svc. Profile	VOIPPhone-StaticIP	Refer to Prerequisites (Profiles and Hard-coded Values).
IP Addr Mask	10.10.144.123 255.255.255.0	Voice Subnet
GenBand Configuration	Line Profile: g711 Interface Group: gr303 (gr303) CRV: 1	format is: name (type)



Provision New Triple Play Customer

Description (Customer ID): Static Customer

iMG/RG General Configuration

iMG/RG General Profile: DeskLab-3Play-1Video iMG/RG MAC Address: 00:0D:DA:00:02:D9

Video/Data Configuration

Access Device: 192.168.42.39 Slot.Port: 10.2 (FE) Port Profile:

Data Svcs. Config: Internet Svc. Profile: HomeNetworkInet-StaticIP

Internet IP Addr: 10.10.2.39 Mask: 255.255.255.192

Local IP Addr: 192.168.0.1 Mask: 255.255.255.252 DHCP Start Addr: 192.168.0.2 DHCP End Addr: 192.168.0.2

Video Service Config: Video Svc. Profile: Video-Flooding

Allowed STB MAC Addrs:

STB #1: STB #2: STB #3:

STB #4: STB #5: STB #6:

Voice Configuration

Derived Voice: Derived Voice Svc. Profile: VOIPPhone-StaticIP IP Addr: 10.10.144.123 Mask: 255.255.255.0

GenBand Configuration:

Port #1: Line Profile: g711 Interface Group: gr303 (gr303) CRV: 1

Port #2: Line Profile: Interface Group: CRV:

Port #3: Line Profile: Interface Group: CRV:

Port #4: Line Profile: Interface Group: CRV:

FIGURE 24-11 Triple Play Form for Static Provisioning

After clicking on Provision, the AlliedView NMS stores all of the values.

If the RG has previously been discovered, the values in the Triple-Play form are applied. If the RG has not been discovered, discovery can be done in two ways:

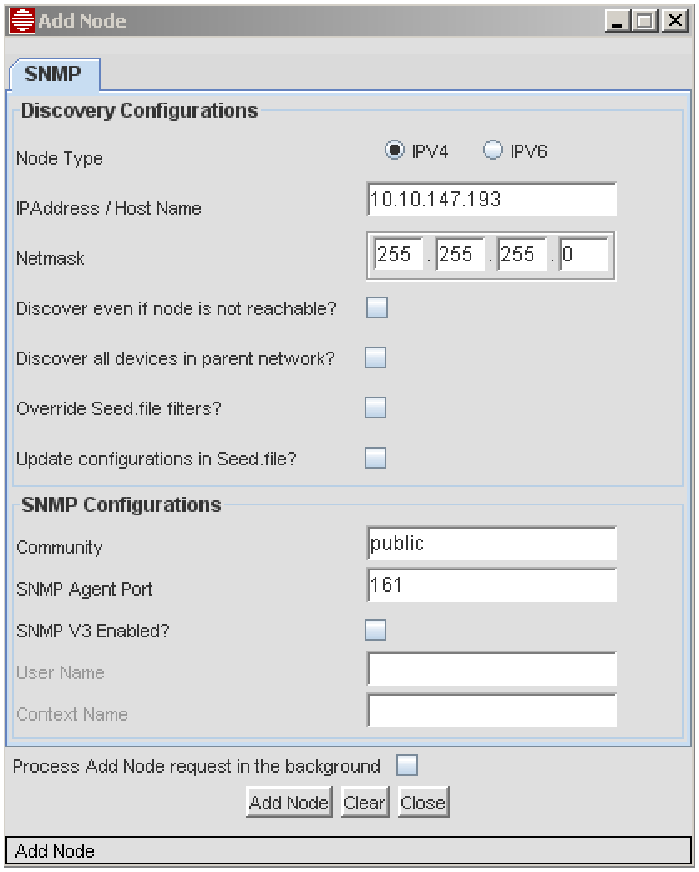
- Wait for the 24-hour discovery cycle to discover the RG. The AlliedView NMS will perform an SNMP ping and eventually ping using the address given to the RG (assuming the AlliedView NMS has discovery set up for the subnet that the manually given IP address belongs to).

Note: *The default Discovery period is 24 hours, assuming there are few enough devices so that in 24 hours all devices can be discovered. If there are a large number of devices, the period will extend beyond 24 hours.*

- Manually add the RG using Add Node, as explained next.

24.3.4 Add the RG to the Network

Selecting *Edit -> Add Node* brings up the Add Node window, as shown in the following figure.



Discovery Configurations

Node Type	● IPV4 ○ IPV6
IPAddress / Host Name	10.10.147.193
Netmask	255 . 255 . 255 . 0
Discover even if node is not reachable?	□
Discover all devices in parent network?	□
Override Seed.file filters?	□
Update configurations in Seed.file?	□

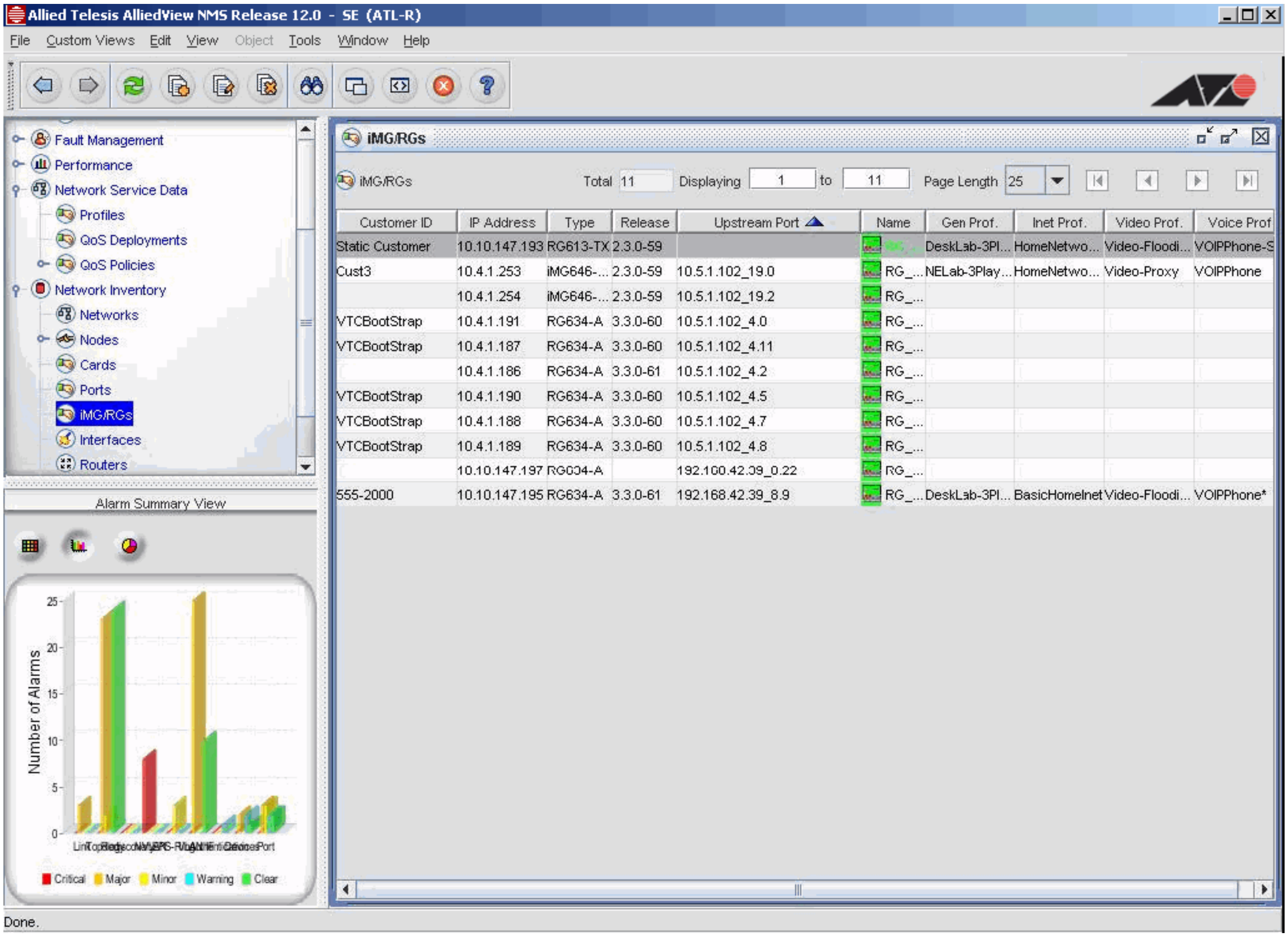
SNMP Configurations

Community	public
SNMP Agent Port	161
SNMP V3 Enabled?	□
User Name	
Context Name	

Process Add Node request in the background □

FIGURE 24-12 Adding the RG to. the Network Manually (Add Node Form)

When the user clicks on **Add Node**, the AlliedView NMS immediately begins configuring the RG. In the iMG/RG table (under Network Inventory), the RG with the ID “Static Customer” at first has no columns filled in since it has not been discovered. Once discovered, the columns begin to fill in. The IP address value from the Add Node form appears, and finally the Profiles appear. Refer to the following figure.



iMG/RGs

iMG/RGs Total 11 Displaying 1 to 11 Page Length 25

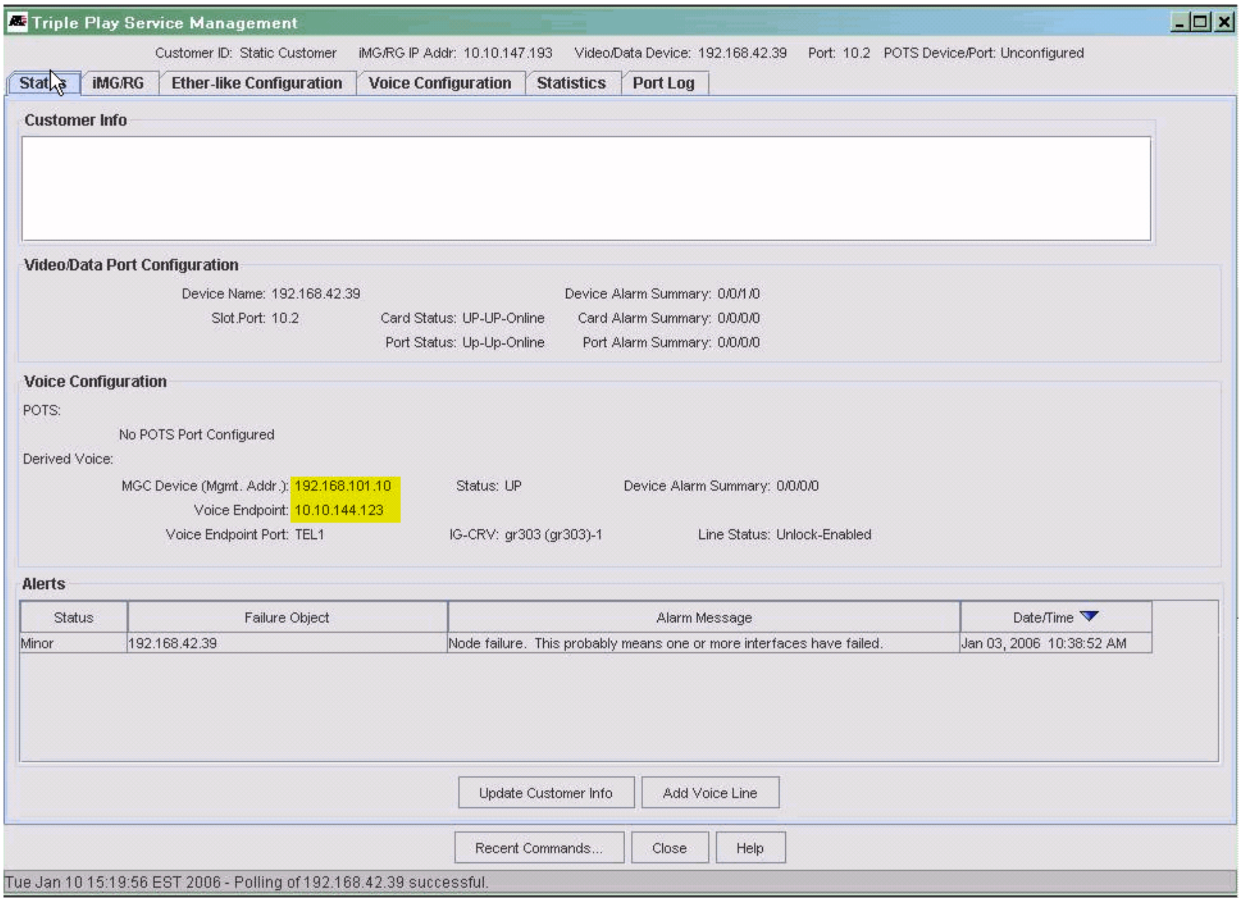
Customer ID	IP Address	Type	Release	Upstream Port	Name	Gen Prof.	Inet Prof.	Video Prof.	Voice Prof
Static Customer	10.10.147.193	RG613-TX	2.3.0-59		[illegible]	DeskLab-3Pl...	HomeNetwo...	Video-Floodi...	VOIPPhone-S
Cust3	10.4.1.253	iMG646-...	2.3.0-59	10.5.1.102_19.0	RG_...	NELab-3Play...	HomeNetwo...	Video-Proxy	VOIPPhone
	10.4.1.254	iMG646-...	2.3.0-59	10.5.1.102_19.2	RG_...				
VTCBootStrap	10.4.1.191	RG634-A	3.3.0-60	10.5.1.102_4.0	RG_...				
VTCBootStrap	10.4.1.187	RG634-A	3.3.0-60	10.5.1.102_4.11	RG_...				
	10.4.1.186	RG634-A	3.3.0-61	10.5.1.102_4.2	RG_...				
VTCBootStrap	10.4.1.190	RG634-A	3.3.0-60	10.5.1.102_4.5	RG_...				
VTCBootStrap	10.4.1.188	RG634-A	3.3.0-60	10.5.1.102_4.7	RG_...				
VTCBootStrap	10.4.1.189	RG634-A	3.3.0-60	10.5.1.102_4.8	RG_...				
	10.10.147.197	RG634-A		192.168.42.39_0.22	RG_...				
555-2000	10.10.147.195	RG634-A	3.3.0-61	192.168.42.39_8.9	RG_...	DeskLab-3Pl...	BasicHomeInet	Video-Floodi...	VOIPPhone*

FIGURE 24-13 Adding RG with Static Values - Discovery Complete

Note that the Upstream Port field is not filled in, since DHCP discovery was not used.

24.3.5 Viewing Static Configuration

Viewing the status windows shows the differences between the statically and dynamically configured iMG/RG. The following figures list the tabbed windows that show these differences.



Customer ID: Static Customer iMG/RG IP Addr: 10.10.147.193 Video/Data Device: 192.168.42.39 Port: 10.2 POTS Device/Port: Unconfigured

Customer Info

Video/Data Port Configuration

Device Name: 192.168.42.39 Device Alarm Summary: 0/0/1/0

Slot.Port: 10.2 Card Status: UP-UP-Online Card Alarm Summary: 0/0/0/0

Port Status: Up-Up-Online Port Alarm Summary: 0/0/0/0

Voice Configuration

POTS:

No POTS Port Configured

Derived Voice:

MGC Device (Mgmt. Addr.): 192.168.101.10 Status: UP Device Alarm Summary: 0/0/0/0

Voice Endpoint: 10.10.144.123

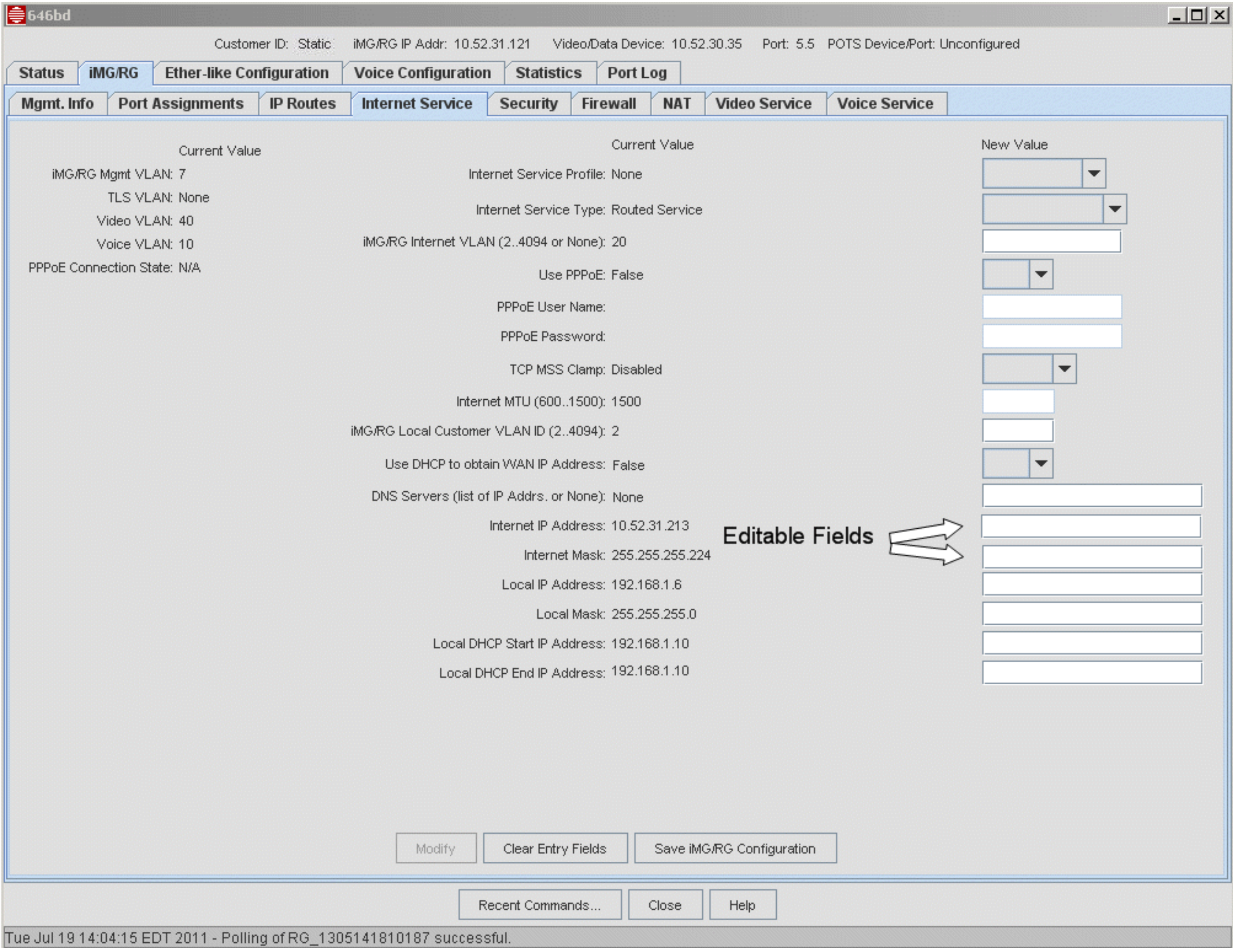
Voice Endpoint Port: TEL1 IG-CRV: gr303 (gr303)-1 Line Status: Unlock-Enabled

Alerts

Status	Failure Object	Alarm Message	Date/Time ▼
Minor	192.168.42.39	Node failure. This probably means one or more interfaces have failed.	Jan 03, 2006 10:38:52 AM

Tue Jan 10 15:19:56 EST 2006 - Polling of 192.168.42.39 successful.

FIGURE 24-14 Static iMG/RG Configuration - Status Tab



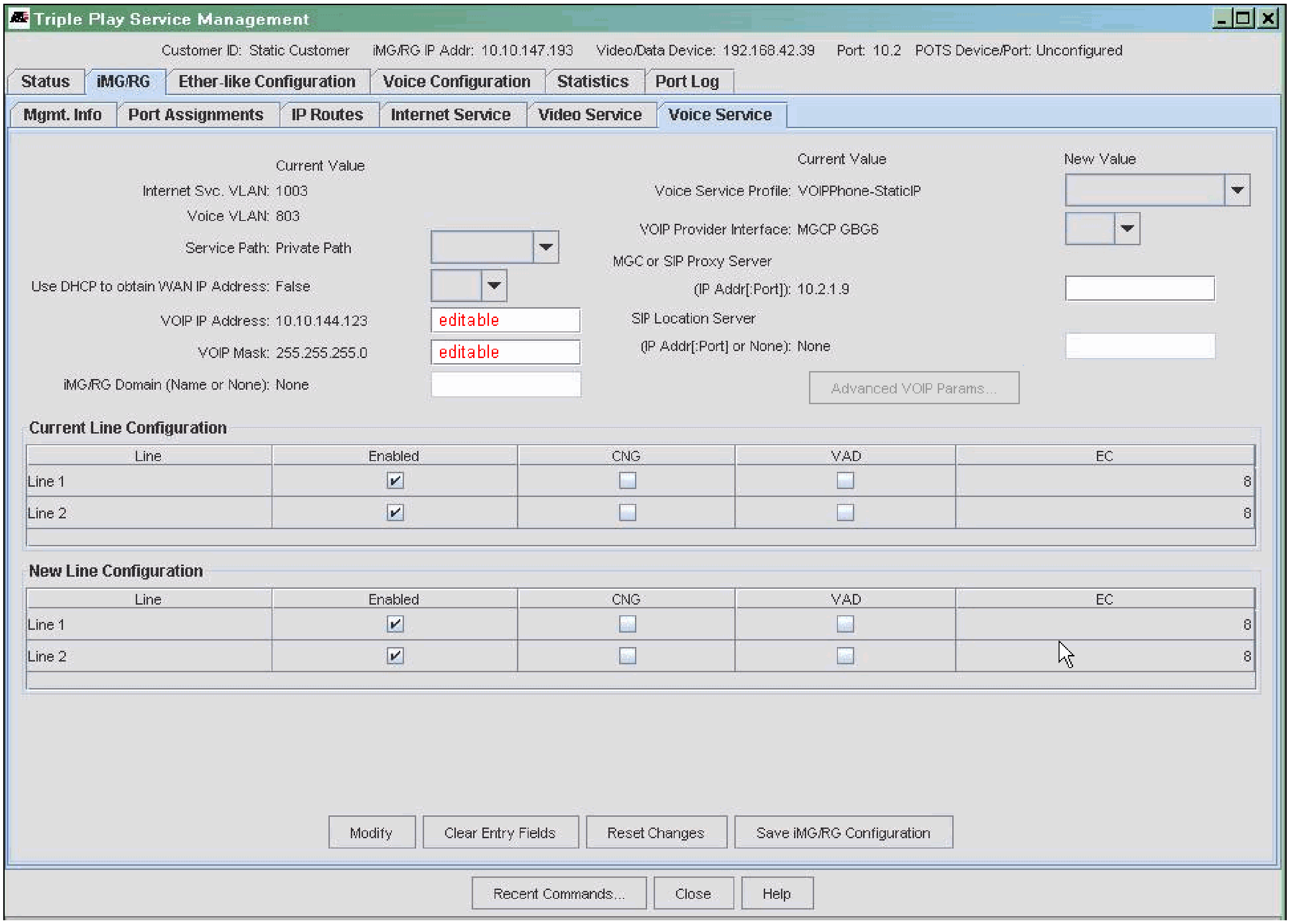
Customer ID: Static iMG/RG IP Addr: 10.52.31.121 Video/Data Device: 10.52.30.35 Port: 5.5 POTS Device/Port: Unconfigured

	Current Value
iMG/RG Mgmt VLAN:	7
TLS VLAN:	None
Video VLAN:	40
Voice VLAN:	10
PPPoE Connection State:	N/A

	Current Value	New Value
Internet Service Profile:	None	
Internet Service Type:	Routed Service	
iMG/RG Internet VLAN (2..4094 or None):	20	
Use PPPoE:	False	
PPPoE User Name:		
PPPoE Password:		
TCP MSS Clamp:	Disabled	
Internet MTU (600..1500):	1500	
iMG/RG Local Customer VLAN ID (2..4094):	2	
Use DHCP to obtain WAN IP Address:	False	
DNS Servers (list of IP Addrs. or None):	None	
Internet IP Address:	10.52.31.213	
Internet Mask:	255.255.255.224	
Local IP Address:	192.168.1.6	
Local Mask:	255.255.255.0	
Local DHCP Start IP Address:	192.168.1.10	
Local DHCP End IP Address:	192.168.1.10	

Tue Jul 19 14:04:15 EDT 2011 - Polling of RG_1305141810187 successful.

FIGURE 24-15 Static iMG/RG Configuration - Internet Service Tab



Customer ID: Static Customer iMG/RG IP Addr: 10.10.147.193 Video/Data Device: 192.168.42.39 Port: 10.2 POTS Device/Port: Unconfigured

	Current Value	New Value
Internet Svc. VLAN:	1003	
Voice VLAN:	803	
Service Path:	Private Path	
Use DHCP to obtain WAN IP Address:	False	
VOIP IP Address:	10.10.144.123	editable
VOIP Mask:	255.255.255.0	editable
iMG/RG Domain (Name or None):	None	

	Current Value	New Value
Voice Service Profile:	VOIPPhone-StaticIP	
VOIP Provider Interface:	MGCP GBG6	
MGC or SIP Proxy Server (IP Addr[:Port]):	10.2.1.9	
SIP Location Server (IP Addr[:Port] or None):	None	

Current Line Configuration

Line	Enabled	CNG	VAD	EC
Line 1	☑	□	□	8
Line 2	☑	□	□	8

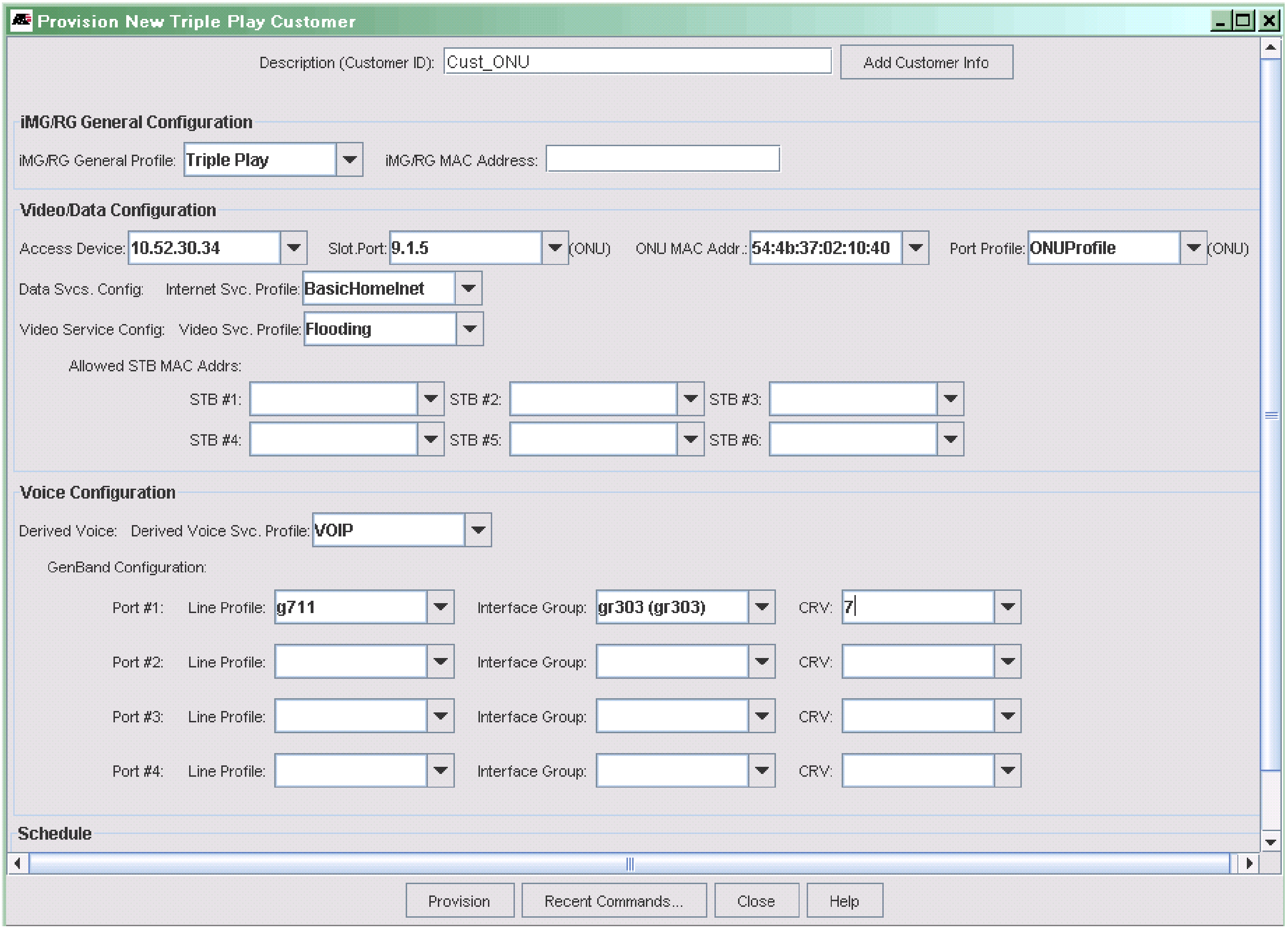
New Line Configuration

Line	Enabled	CNG	VAD	EC
Line 1	☑	□	□	8
Line 2	☑	□	□	8

FIGURE 24-16 Static iMG/RG Configuration - Voice Service Tab

24.4 Configuration 4 - EPON/ONU Interface Connected with iMG646PX-ON

This example is similar to the first two examples, but the use of Profiles is highlighted because of the use of EPON/ONU specific QoS policies, as explained in Example of an EPON/ONU Interface Policy.



Description (Customer ID): Cust_ONU

iMG/RG General Profile: Triple Play

Access Device: 10.52.30.34

Slot.Port: 9.1.5 (ONU)

ONU MAC Addr.: 54:4b:37:02:10:40

Port Profile: ONUProfile (ONU)

Internet Svc. Profile: BasicHomeInet

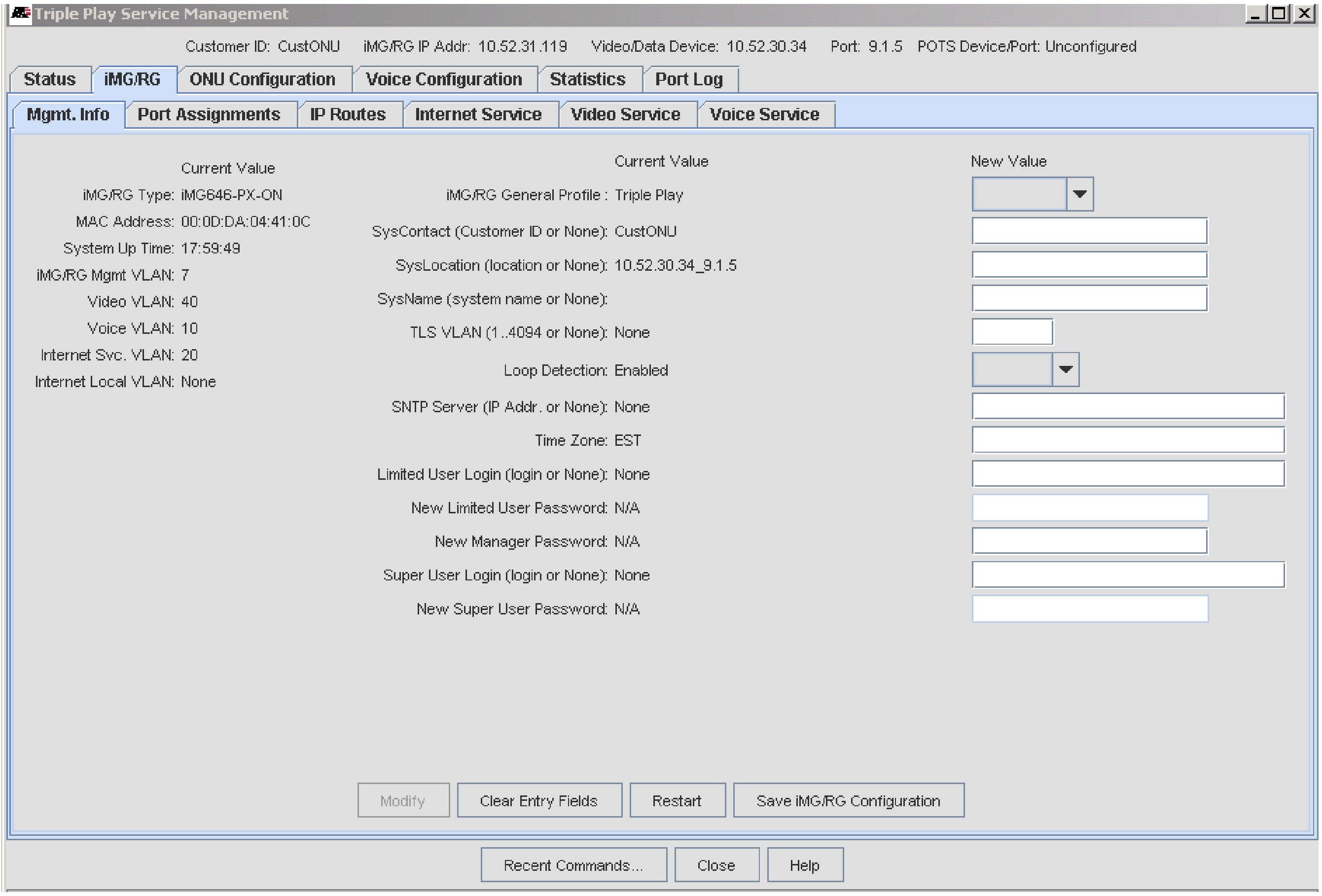
Video Svc. Profile: Flooding

Derived Voice Svc. Profile: VOIP

Port #1: Line Profile: g711 Interface Group: gr303 (gr303) CRV: 7

FIGURE 24-17 Triple-Play for the EPON/ONU

Figure 24-17 shows the Triple-Play form when filled out for the ONU interface. The main differences are the ONU interface format (the EPON slot.port and ONU logical ID) and the MAC address for the ONU.



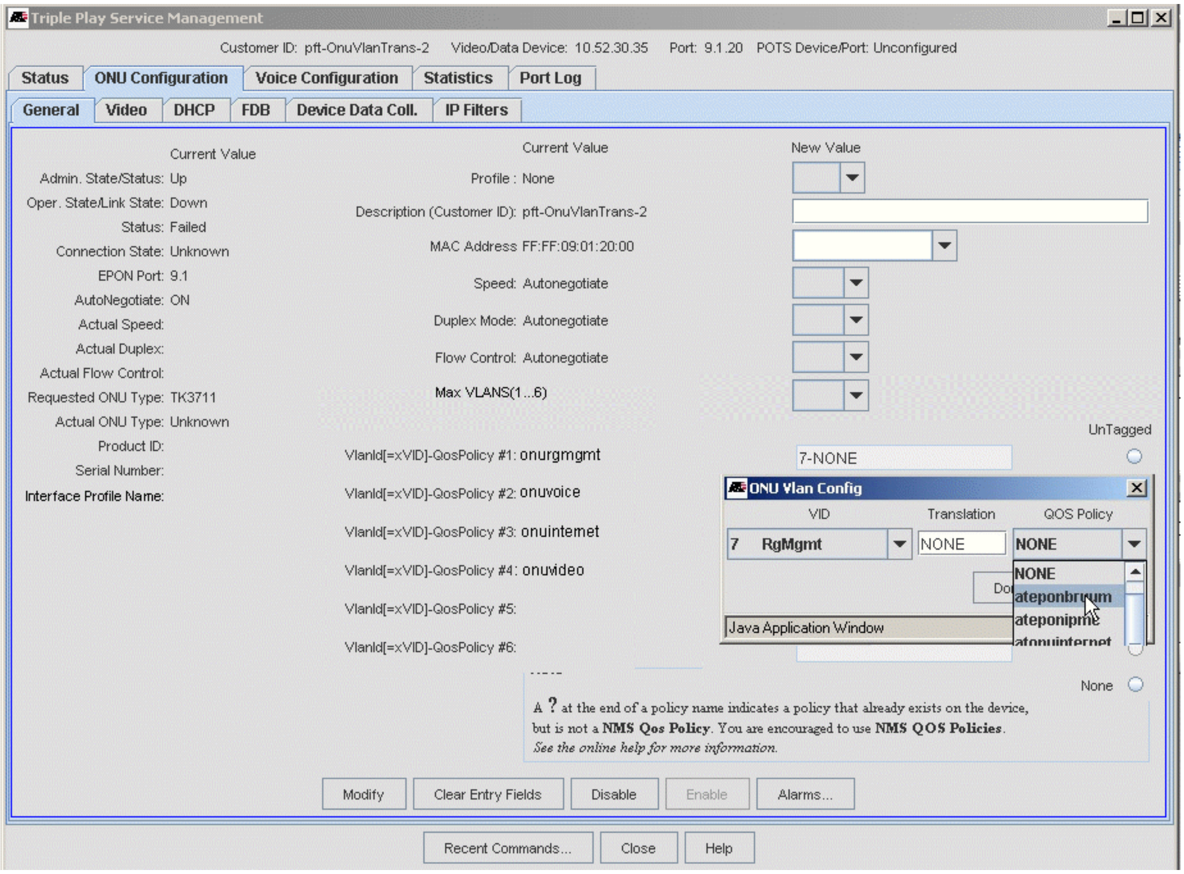
Customer ID: CustONU iMG/RG IP Addr: 10.52.31.119 Video/Data Device: 10.52.30.34 Port: 9.1.5 POTS Device/Port: Unconfigured

Current Value
iMG/RG Type: iMG646-PX-ON
MAC Address: 00:0D:DA:04:41:0C
System Up Time: 17:59:49
iMG/RG Mgmt VLAN: 7
Video VLAN: 40
Voice VLAN: 10
Internet Svc. VLAN: 20
Internet Local VLAN: None

Current Value
iMG/RG General Profile : Triple Play
SysContact (Customer ID or None): CustONU
SysLocation (location or None): 10.52.30.34_9.1.5
SysName (system name or None):
TLS VLAN (1..4094 or None): None
Loop Detection: Enabled
SNTP Server (IP Addr. or None): None
Time Zone: EST
Limited User Login (login or None): None
New Limited User Password: N/A
New Manager Password: N/A
Super User Login (login or None): None
New Super User Password: N/A

FIGURE 24-18 Service Management Window -> iMG/RG Tab for EPON/ONU

Figure 24-18 shows the Service Management Form once the iMG/RG is configured. The iMG/RG-> Mgmt. Info tab provides a summary of all the main attributes.



Triple Play Service Management

Customer ID: pft-OnuVlanTrans-2 Video/Data Device: 10.52.30.35 Port: 9.1.20 POTS Device/Port: Unconfigured

Current Value
Admin. State/Status: Up
Oper. State/Link State: Down
Status: Failed
Connection State: Unknown
EPON Port: 9.1
AutoNegotiate: ON
Actual Speed:
Actual Duplex:
Actual Flow Control:
Requested ONU Type: TK3711
Actual ONU Type: Unknown
Product ID:
Serial Number:
Interface Profile Name:

Current Value New Value
Profile : None
Description (Customer ID): pft-OnuVlanTrans-2
MAC Address FF:FF:09:01:20:00
Speed: Autonegotiate
Duplex Mode: Autonegotiate
Flow Control: Autonegotiate
Max VLANS(1...6)
VlanId[=xVID]-QosPolicy #1: onurgmgmt 7-NONE
VlanId[=xVID]-QosPolicy #2: onuvoice
VlanId[=xVID]-QosPolicy #3: onuinternet
VlanId[=xVID]-QosPolicy #4: onuvideo
VlanId[=xVID]-QosPolicy #5:
VlanId[=xVID]-QosPolicy #6:

UnTagged ○
None ○

ONU Vlan Config

VID	Translation	QOS Policy
7 RgMgmt	NONE	NONE

A ? at the end of a policy name indicates a policy that already exists on the device, but is not a **NMS Qos Policy**. You are encouraged to use **NMS QOS Policies**. *See the online help for more information.*

FIGURE 24-19 Service Management Window -> ONU Configuration Tab for EPON/ONU

Figure 24-19 shows the Service Management Form with the ONU Configuration tab. On this form the user can change the VLAN-QoS policy association. The available VLANs and policies are included in the pull-down menus.

Note: The EPON supports translations. When the user clicks on the New Value field for the VLAN Info, a pop-up includes the VID, translation, and QOS Policy that are to be associated. These are the same values that can be datafilled with the ONU profile. As with other profiles, the user should be aware that if the ONU was configured with a profile and changes are made here, the ONU will be out of sync with the Profile.

24.5 Configuration 5 - Voice Service Provided by SIP

Configuration 5 is similar to Configuration 1, but in this example the voice service is provided by SIP. Refer to the following figure.

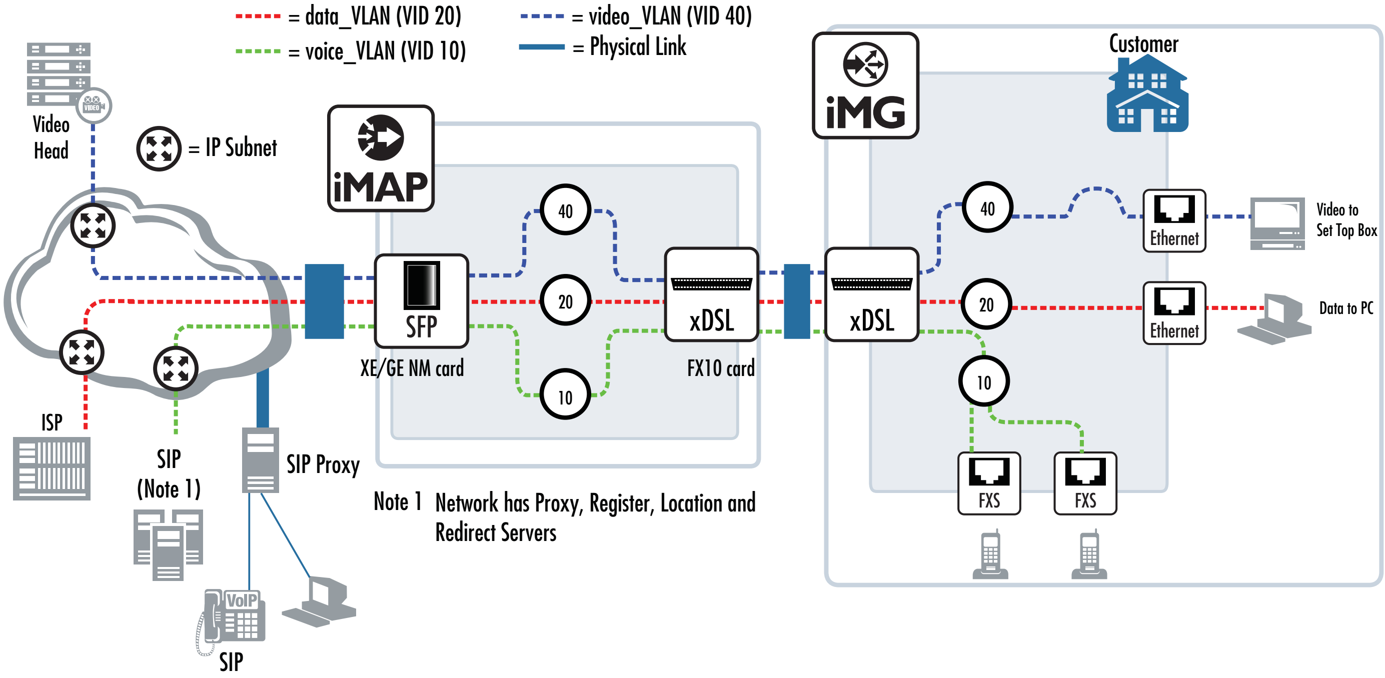
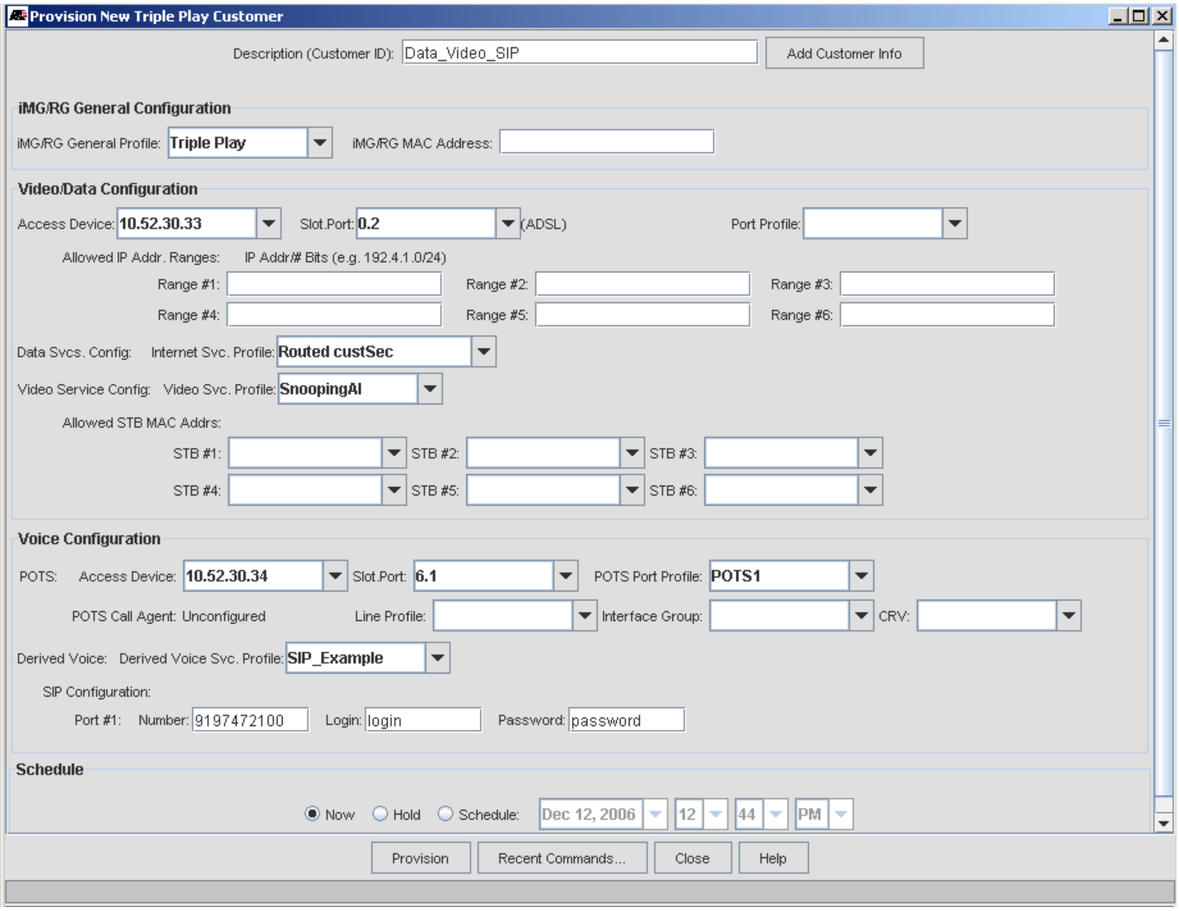


FIGURE 24-20 Configuration 5 - VoIP using SIP

Note: *This example is included because a phone is included that connects to the SIP network using the POTS24 that has been configured to support SIP.*

Refer to the following figure to show how the Triple Play form is filled out to support SIP.



Description (Customer ID): Data_Video_SIP

iMG/RG General Configuration

iMG/RG General Profile: Triple Play iMG/RG MAC Address:

Video/Data Configuration

Access Device: 10.52.30.33 Slot.Port: 0.2 (ADSL) Port Profile:

Allowed IP Addr. Ranges: IP Addr/# Bits (e.g. 192.4.1.0/24)

Range #1: Range #2: Range #3:

Range #4: Range #5: Range #6:

Data Svcs. Config: Internet Svc. Profile: Routed custSec

Video Service Config: Video Svc. Profile: SnoopingAl

Allowed STB MAC Addrs:

STB #1: STB #2: STB #3:

STB #4: STB #5: STB #6:

Voice Configuration

POTS: Access Device: 10.52.30.34 Slot.Port: 6.1 POTS Port Profile: POTS1

POTS Call Agent: Unconfigured Line Profile: Interface Group: CRV:

Derived Voice: Derived Voice Svc. Profile: SIP_Example

SIP Configuration:

Port #1: Number: 9197472100 Login: login Password: password

Schedule

● Now ○ Hold ○ Schedule: Dec 12, 2006 12 44 PM

FIGURE 24-21 Triple Play Form with SIP for Voice

24.6 Configuration 6 - Multi-Service VLAN

Configuration 6 involves placing more than one service on a VLAN.

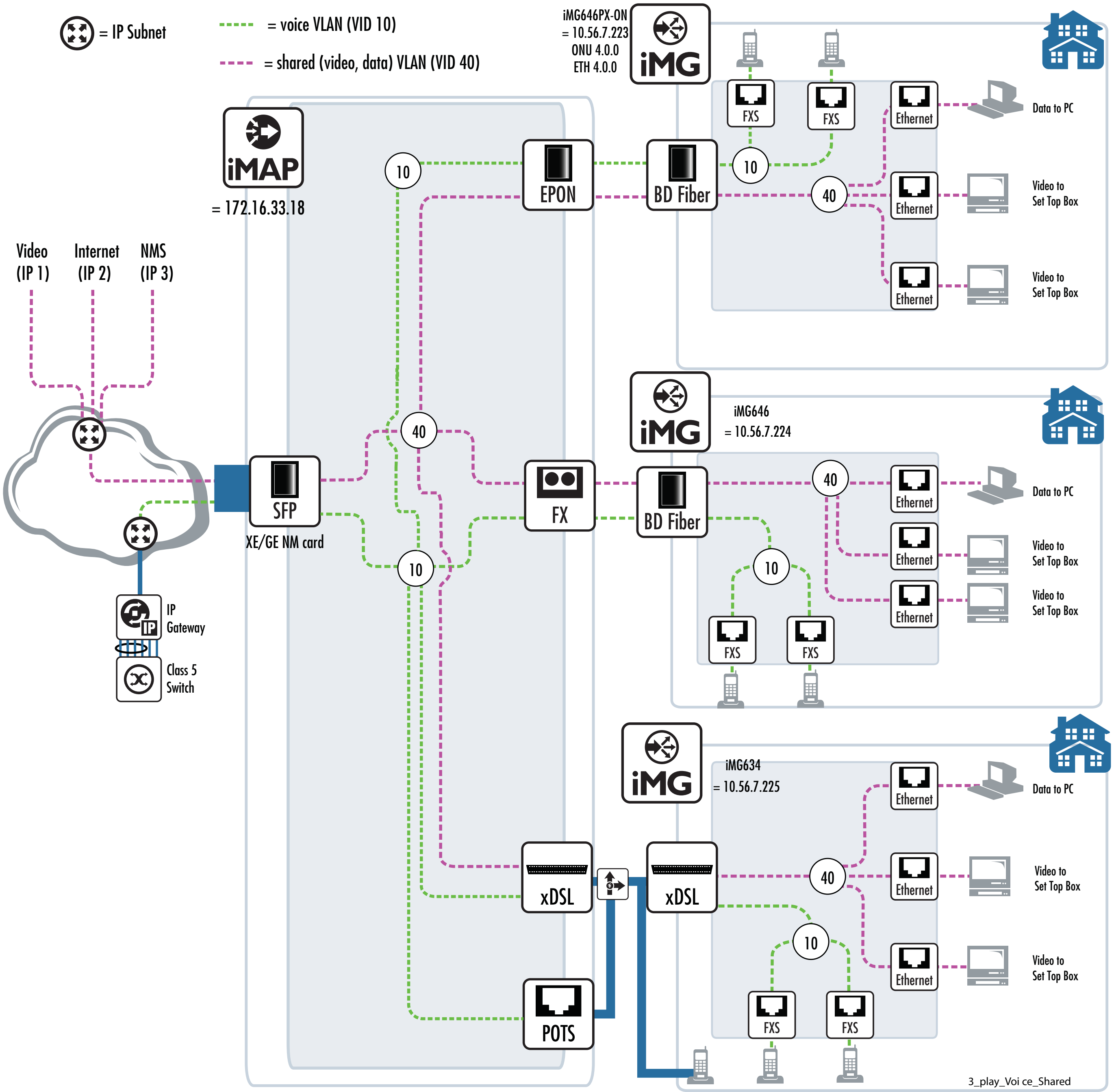
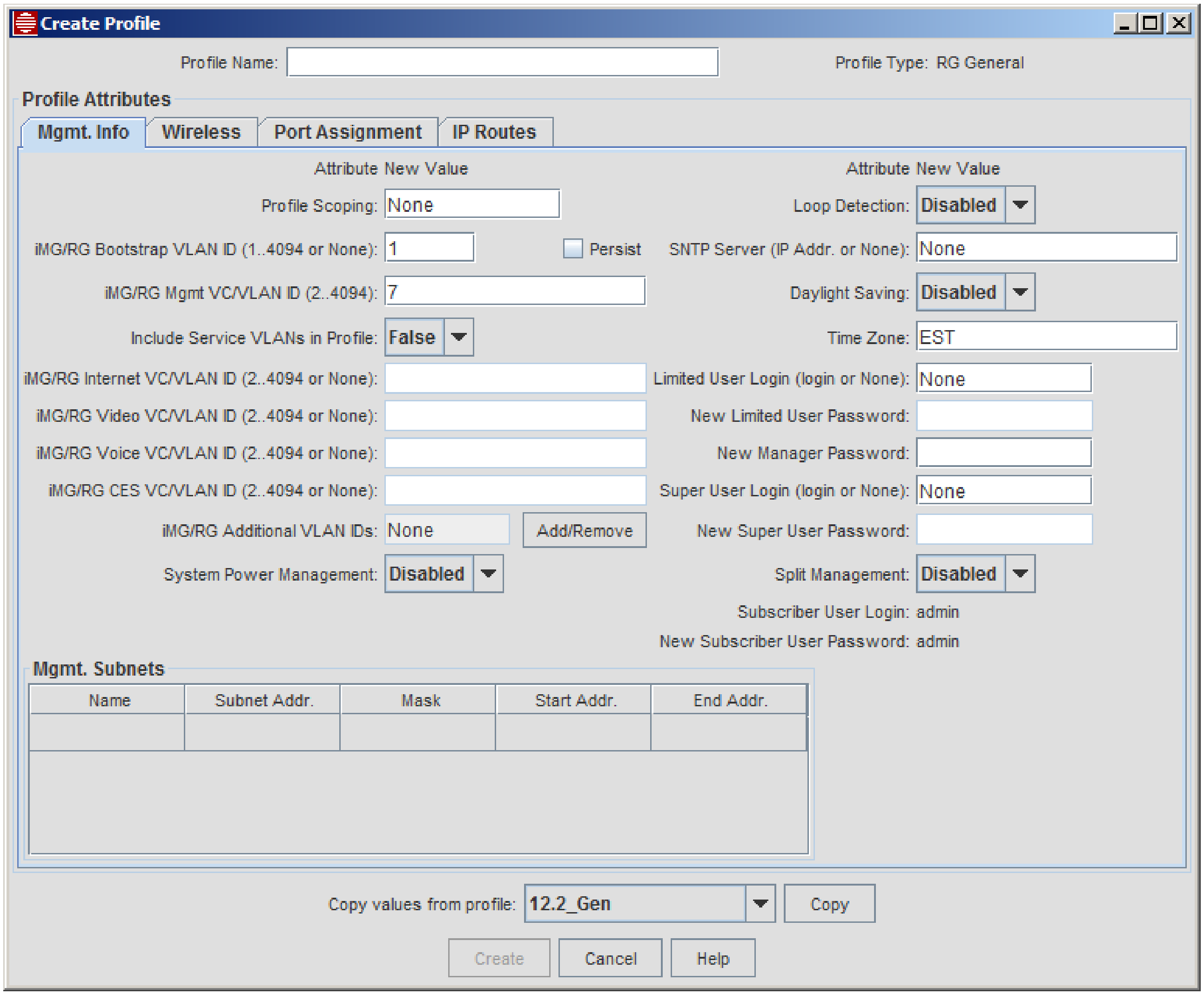


FIGURE 24-22 Configuration 6 - Multi-Service VLAN

24.6.1 RG Forms



Profile Name:

Profile Type: RG General

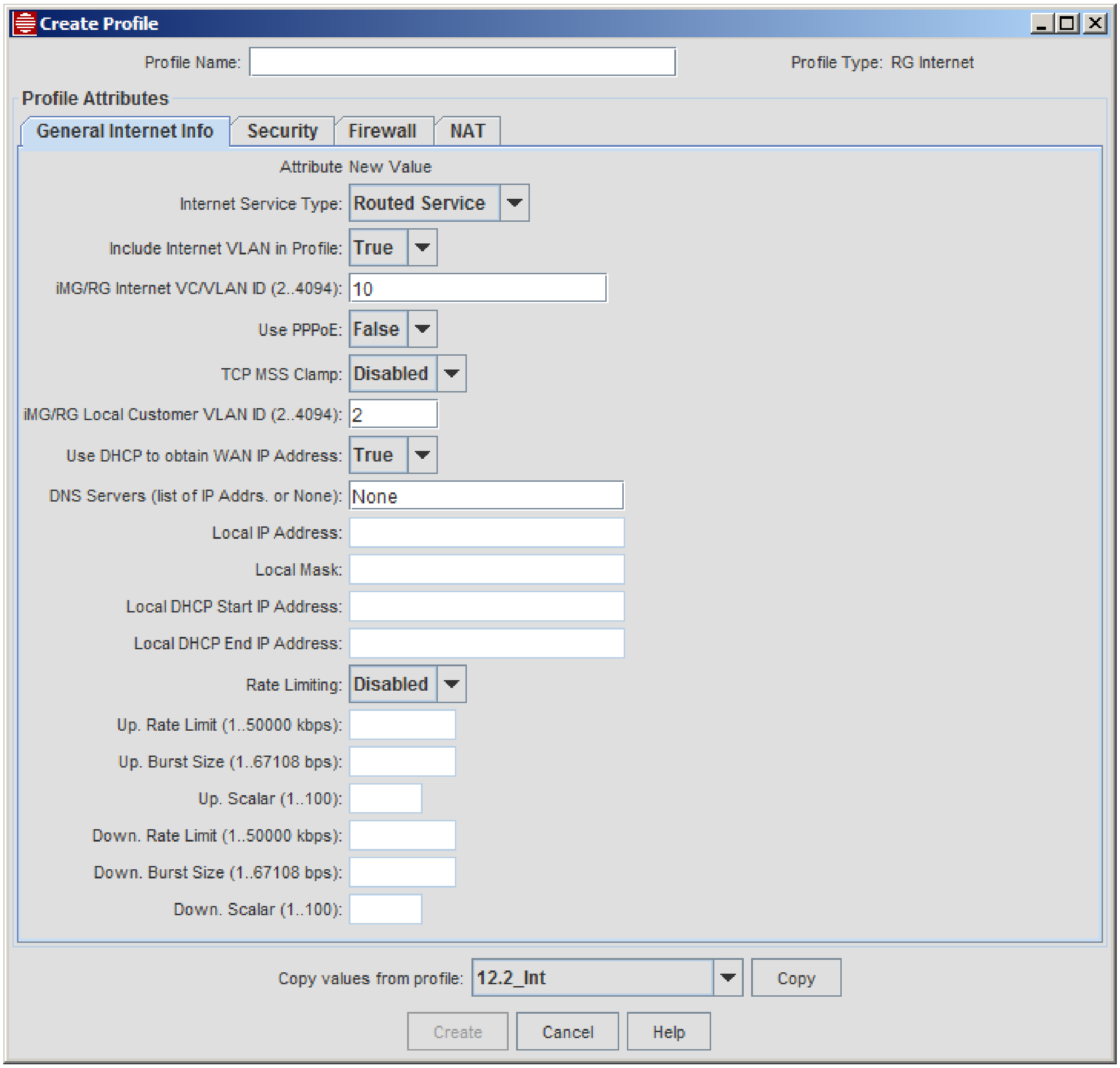
Attribute	New Value	Attribute	New Value
Profile Scoping:	None	Loop Detection:	Disabled
iMG/RG Bootstrap VLAN ID (1..4094 or None):	1 □ Persist	SNTP Server (IP Addr. or None):	None
iMG/RG Mgmt VC/VLAN ID (2..4094):	7	Daylight Saving:	Disabled
Include Service VLANs in Profile:	False	Time Zone:	EST
iMG/RG Internet VC/VLAN ID (2..4094 or None):		Limited User Login (login or None):	None
iMG/RG Video VC/VLAN ID (2..4094 or None):		New Limited User Password:	
iMG/RG Voice VC/VLAN ID (2..4094 or None):		New Manager Password:	
iMG/RG CES VC/VLAN ID (2..4094 or None):		Super User Login (login or None):	None
iMG/RG Additional VLAN IDs:	None	New Super User Password:	
System Power Management:	Disabled	Split Management:	Disabled
		Subscriber User Login:	admin
		New Subscriber User Password:	admin

Mgmt. Subnets

Name	Subnet Addr.	Mask	Start Addr.	End Addr.

Copy values from profile: 12.2_Gen

FIGURE 24-23 Shared VLAN - RG General - Mgmt. Info



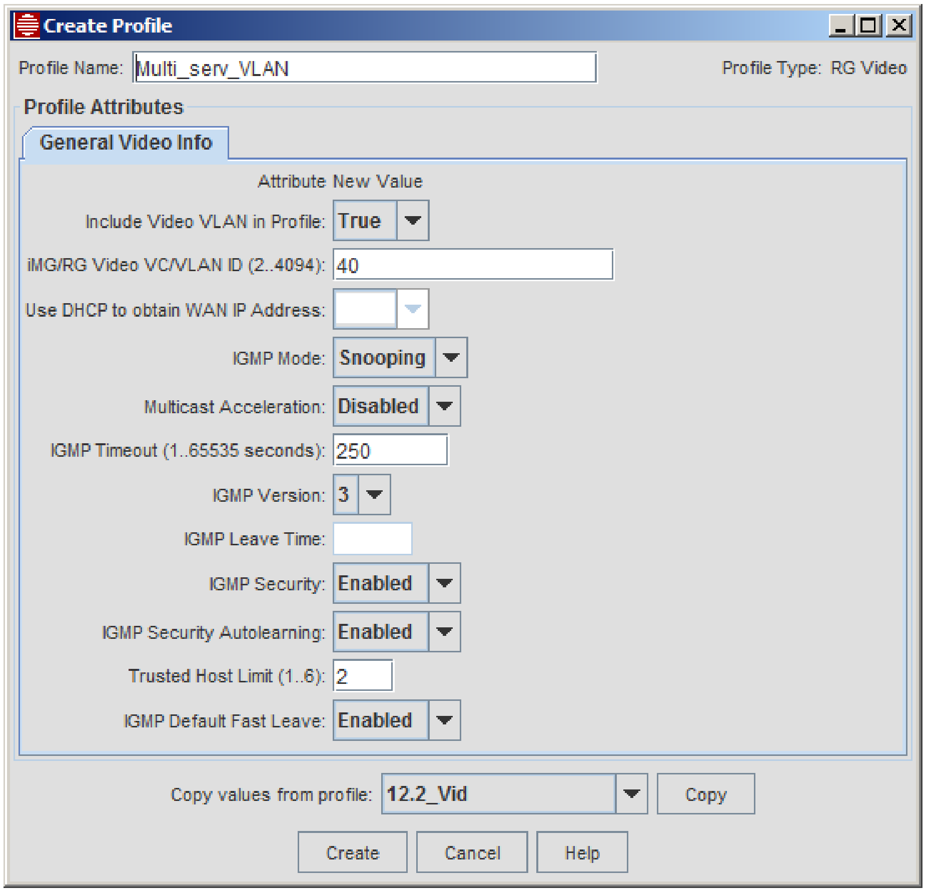
Profile Name:	
Profile Type:	RG Internet

Profile Attributes

Attribute	New Value
Internet Service Type:	Routed Service
Include Internet VLAN in Profile:	True
iMG/RG Internet VC/VLAN ID (2..4094):	10
Use PPPoE:	False
TCP MSS Clamp:	Disabled
iMG/RG Local Customer VLAN ID (2..4094):	2
Use DHCP to obtain WAN IP Address:	True
DNS Servers (list of IP Addrs. or None):	None
Local IP Address:	
Local Mask:	
Local DHCP Start IP Address:	
Local DHCP End IP Address:	
Rate Limiting:	Disabled
Up. Rate Limit (1..50000 kbps):	
Up. Burst Size (1..67108 bps):	
Up. Scalar (1..100):	
Down. Rate Limit (1..50000 kbps):	
Down. Burst Size (1..67108 bps):	
Down. Scalar (1..100):	

Copy values from profile: 12.2_Int

FIGURE 24-24 Multi-service VLAN - Internet - General Profile



Profile Name: Multi_serv_VLAN

Profile Type: RG Video

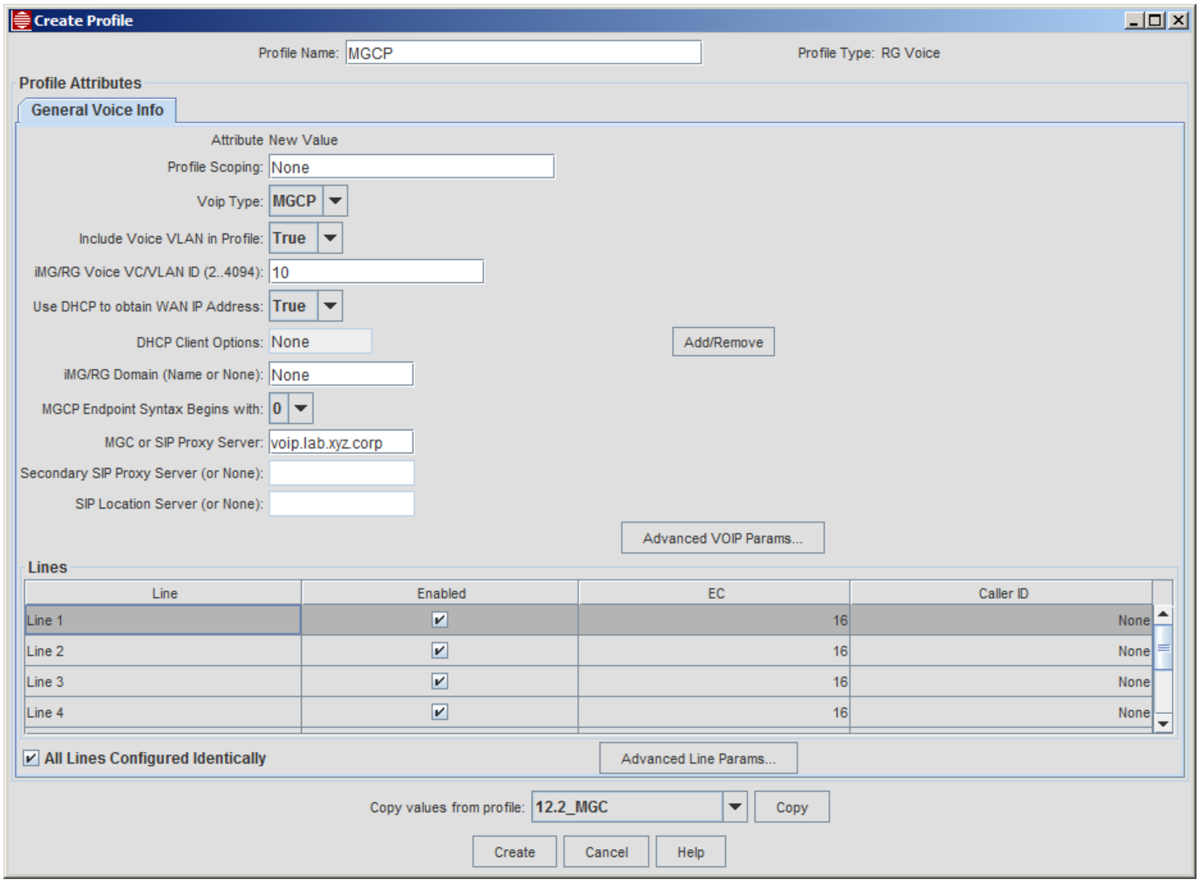
Profile Attributes

General Video Info

Attribute	New Value
Include Video VLAN in Profile:	True
iMG/RG Video VC/VLAN ID (2..4094):	40
Use DHCP to obtain WAN IP Address:	
IGMP Mode:	Snooping
Multicast Acceleration:	Disabled
IGMP Timeout (1..65535 seconds):	250
IGMP Version:	3
IGMP Leave Time:	
IGMP Security:	Enabled
IGMP Security Autolearning:	Enabled
Trusted Host Limit (1..6):	2
IGMP Default Fast Leave:	Enabled

Copy values from profile: 12.2_Vid

FIGURE 24-25 Multi-service VLAN - Video Profile



Create Profile

Profile Name: MGCP

Profile Type: RG Voice

Profile Attributes

General Voice Info

Attribute	New Value
Profile Scoping:	None
Voip Type:	MGCP
Include Voice VLAN in Profile:	True
iMG/RG Voice VC/VLAN ID (2..4094):	10
Use DHCP to obtain WAN IP Address:	True
DHCP Client Options:	None
iMG/RG Domain (Name or None):	None
MGCP Endpoint Syntax Begins with:	0
MGC or SIP Proxy Server:	voip.lab.xyz.corp
Secondary SIP Proxy Server (or None):	
SIP Location Server (or None):	

Lines

Line	Enabled	EC	Caller ID
Line 1	☑	16	None
Line 2	☑	16	None
Line 3	☑	16	None
Line 4	☑	16	None

☑ All Lines Configured Identically

Copy values from profile: 12.2_MGC

FIGURE 24-26 Multi-service VLAN - Voice Profile

24.7 Configuration 7 - iMG7x6MOD with HPNA

The iMG7x6MOD can be configured using the RG forms. Moreover, VLAN translation may be needed to ensure the iMG can be integrated into the network.

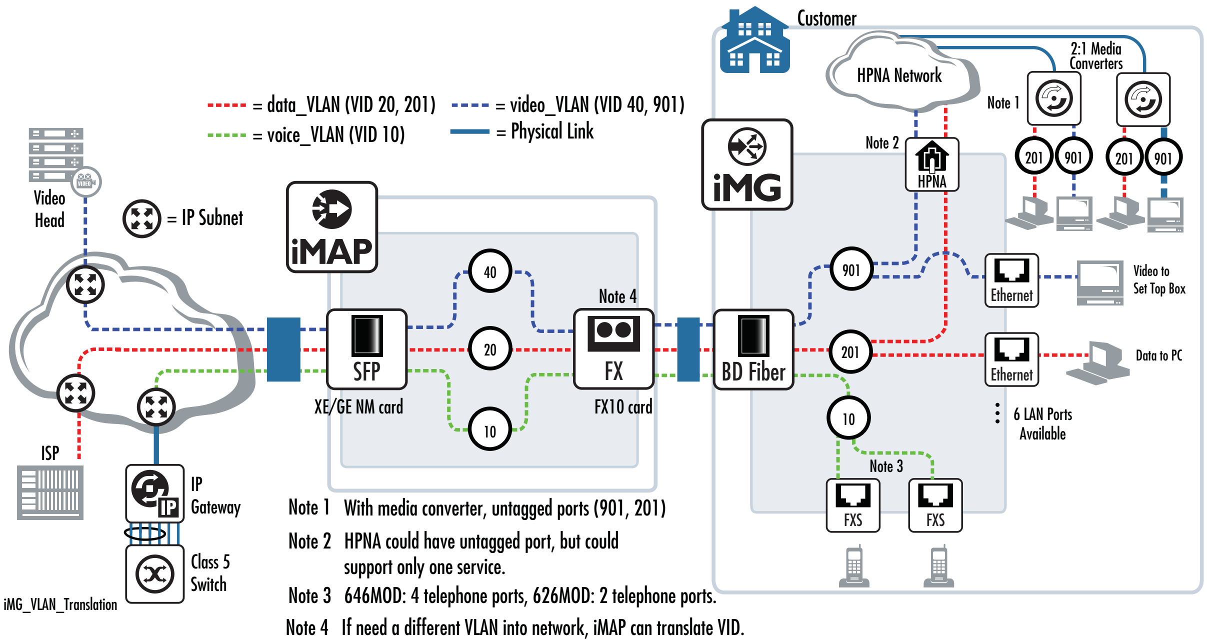

= data_VLAN (VID 20, 201)
= voice_VLAN (VID 10)
= video_VLAN (VID 40, 901)
= Physical Link
= IP Subnet
Video Head
ISP
IP Gateway
Class 5 Switch
iMG_VLAN_Translation
iMAP
SFP
XE/GE NM card
40
20
10
Note 4
FX
FX10 card
iMG
BD Fiber
Customer
HPNA Network
2:1 Media Converters
Note 1
Note 2
HPNA
201
901
Ethernet
Video to Set Top Box
Data to PC
6 LAN Ports Available
Note 3
FXS
Note 1 With media converter, untagged ports (901, 201)
Note 2 HPNA could have untagged port, but could support only one service.
Note 3 646MOD: 4 telephone ports, 626MOD: 2 telephone ports.
Note 4 If need a different VLAN into network, iMAP can translate VID.

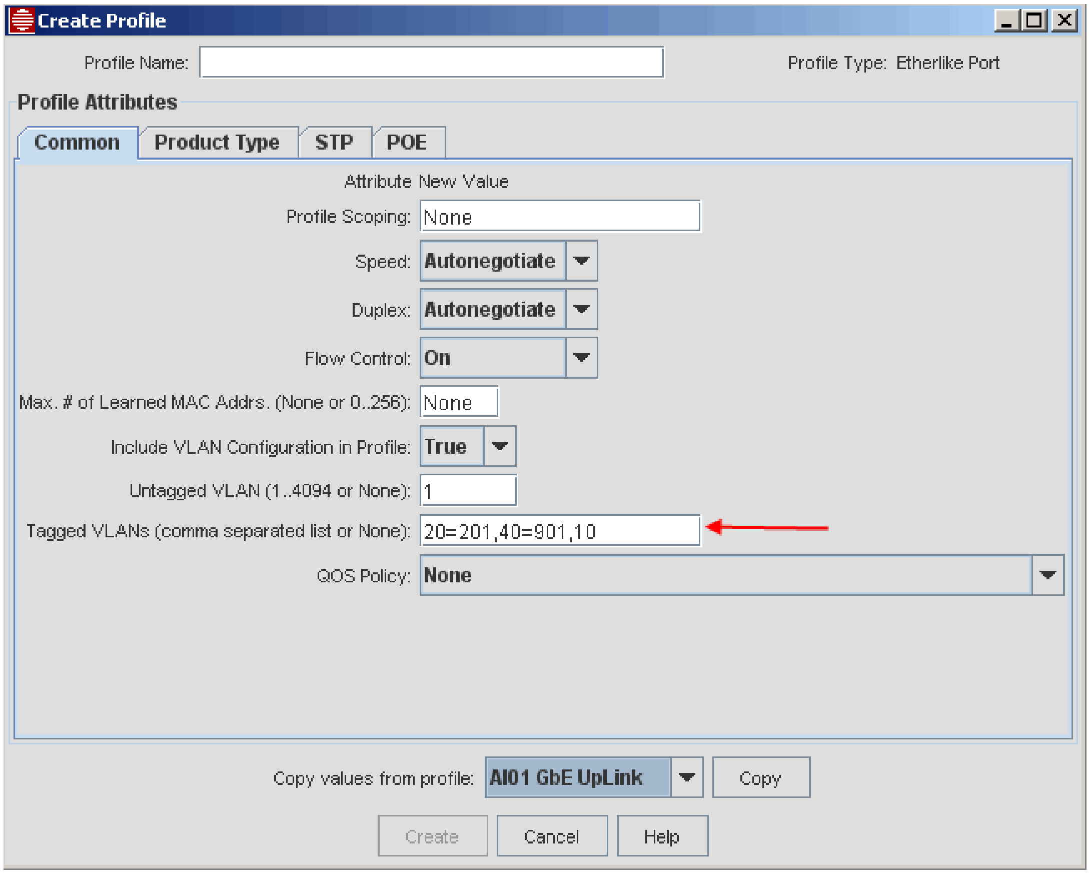
FIGURE 24-27 Configuration 7 - iMG6x6MOD

24.7.1 RG Forms

The iMG6x6MOD product, when using the HPNA LAN interface card, can have devices connected to the residence coax network. Since there is now a set of devices associated with the HPNA as well as the LAN ports, the user must ensure that the VLAN configuration matches the system configuration. Moreover, the media converter used between the coax and ethernet interfaces has untagged VLANs on the ethernet interfaces, numbered 201 and 901. The VLANs used on the LAN ports must also have these two VIDs configured.

Note: The HPNA could also be configured to support an untagged VLAN, but this needs to be configured on the default VLAN (1), and the HPNA could support only one service.

Since the upstream network might not be using VLANs 201 and 901 as their VLANs for data and video, the VLAN must be translated to another VID that matches what the network is using. In release 10.0, this translation feature for iMAP interfaces is available on the Port Profile Form. Refer to Figure 24-28.



Profile Name:

Profile Type: Etherlike Port

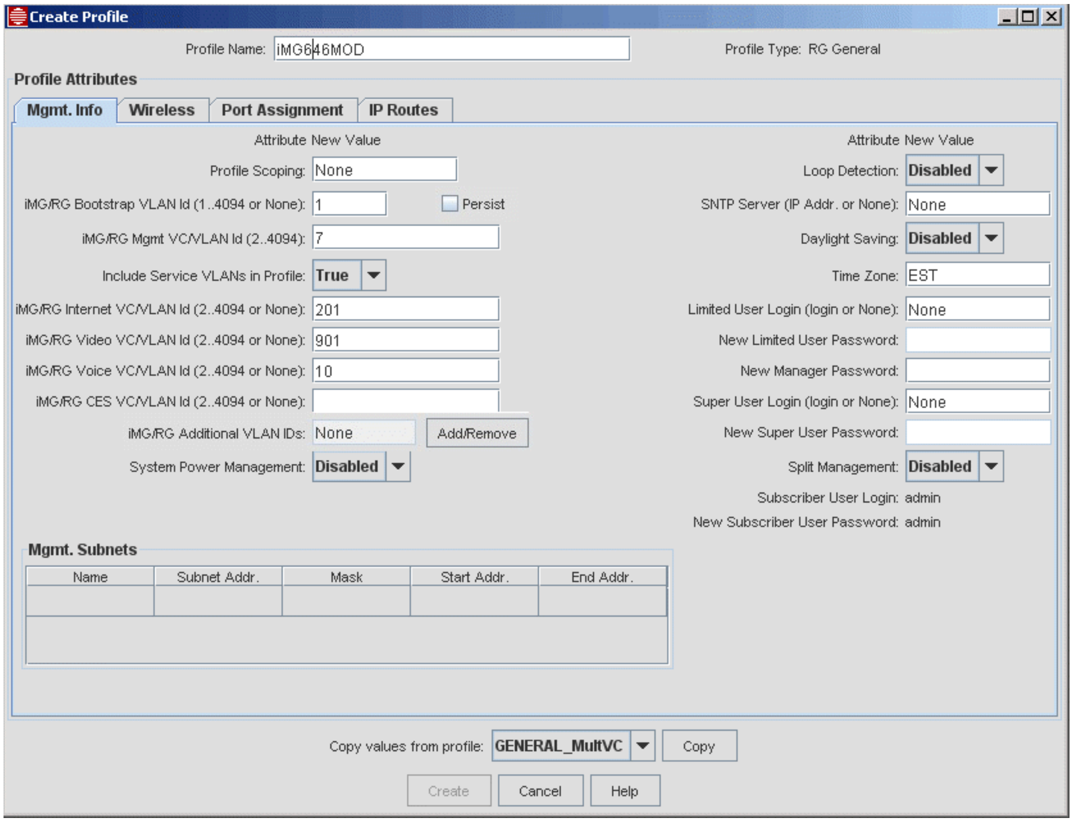
Profile Attributes

Profile Scoping:	None
Speed:	Autonegotiate
Duplex:	Autonegotiate
Flow Control:	On
Max. # of Learned MAC Addrs. (None or 0..256):	None
Include VLAN Configuration in Profile:	True
Untagged VLAN (1..4094 or None):	1
Tagged VLANs (comma separated list or None):	20=201,40=901,10
QOS Policy:	None

Copy values from profile: AI01 GbE UpLink

FIGURE 24-28 Ethernet Port Profile for VLAN Translation (20=201,40=901,10)

Note that when provisioning the iMG Profiles, the user does **not** include any translation information. For example, the RG General profile could be filled out as in Figure 24-29.



Profile Name: iMG646MOD

Profile Type: RG General

Profile Attributes

Attribute	New Value
Profile Scoping:	None
iMG/RG Bootstrap VLAN Id (1..4094 or None):	1 ☐ Persist
iMG/RG Mgmt VC/VLAN Id (2..4094):	7
Include Service VLANs in Profile:	True
iMG/RG Internet VC/VLAN Id (2..4094 or None):	201
iMG/RG Video VC/VLAN Id (2..4094 or None):	901
iMG/RG Voice VC/VLAN Id (2..4094 or None):	10
iMG/RG CES VC/VLAN Id (2..4094 or None):	
iMG/RG Additional VLAN IDs:	None
System Power Management:	Disabled

Attribute	New Value
Loop Detection:	Disabled
SNTP Server (IP Addr. or None):	None
Daylight Saving:	Disabled
Time Zone:	EST
Limited User Login (login or None):	None
New Limited User Password:	
New Manager Password:	
Super User Login (login or None):	None
New Super User Password:	
Split Management:	Disabled
Subscriber User Login:	admin
New Subscriber User Password:	admin

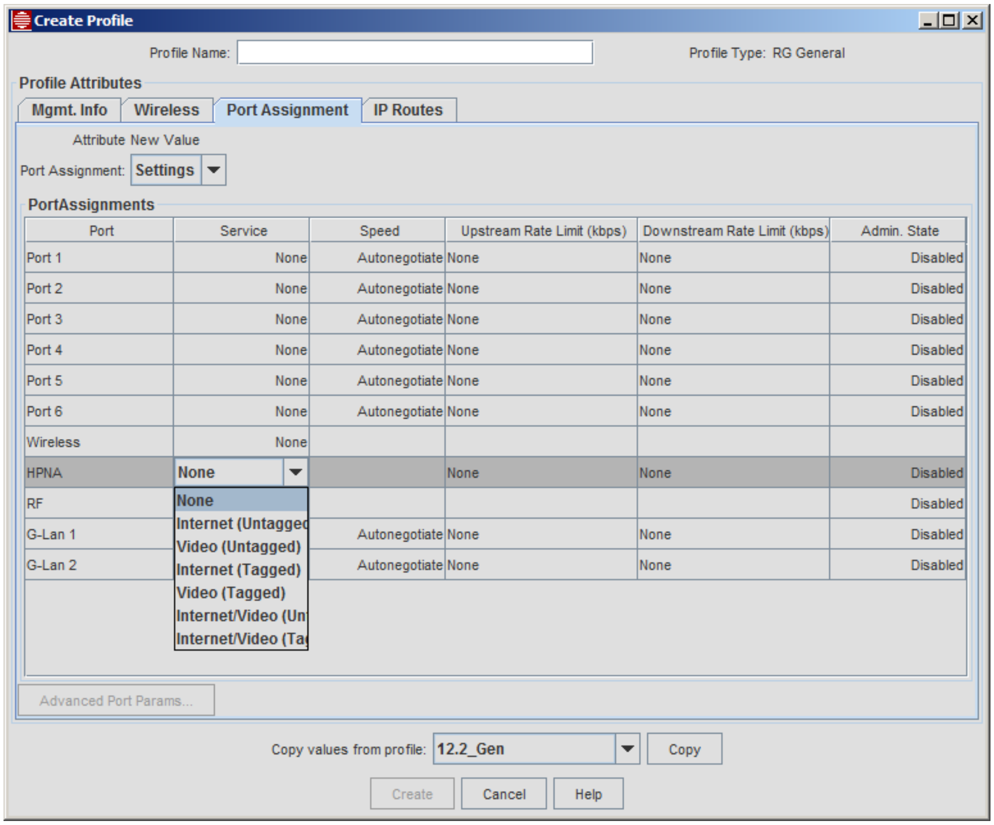
Mgmt. Subnets

Name	Subnet Addr.	Mask	Start Addr.	End Addr.

Copy values from profile: GENERAL_MultVC

FIGURE 24-29 RG General Profile for iMG646MOD (No translations datafilled)

For the HPNA, the Port Assignment tab includes the HPNA port, with the options as shown in Figure 24-30 and Table 24-4.



Profile Name:

Profile Type: RG General

Attribute New Value

Port Assignment: Settings

PortAssignments

Port	Service	Speed	Upstream Rate Limit (kbps)	Downstream Rate Limit (kbps)	Admin. State
Port 1	None	Autonegotiate	None	None	Disabled
Port 2	None	Autonegotiate	None	None	Disabled
Port 3	None	Autonegotiate	None	None	Disabled
Port 4	None	Autonegotiate	None	None	Disabled
Port 5	None	Autonegotiate	None	None	Disabled
Port 6	None	Autonegotiate	None	None	Disabled
Wireless	None				
HPNA	None		None	None	Disabled
RF					Disabled
G-Lan 1		Autonegotiate	None	None	Disabled
G-Lan 2		Autonegotiate	None	None	Disabled

- None
- Internet (Untagged
- Video (Untagged)
- Internet (Tagged)
- Video (Tagged)
- Internet/Video (Un
- Internet/Video (Ta

Copy values from profile: 12.2_Gen

FIGURE 24-30 RG Profile - Port Assignment for HPNA

TABLE 24-4 Provisioning the iMG/RG

Pull-down Option	Description
Internet (Untagged)	The HPNA can support only internet service
Video (Untagged)	The HPNA can support only video service
Internet (Tagged)	The HPNA supports internet service, but could support video service as well.
Video (Tagged)	The HPNA supports video service, but could support internet service as well.
Internet/Video (Tagged)	The HPNA supports both services.

24.8 Configuration 8 - AlliedWare Plus Device

The iMG/RG can be configured with AlliedWare Plus upstream devices (x908, x600, x900) in the same way as iMAP ports (all components provisionable, pre-provisioning so that iMG/RG comes into service automatically).

Following is an example configuration.

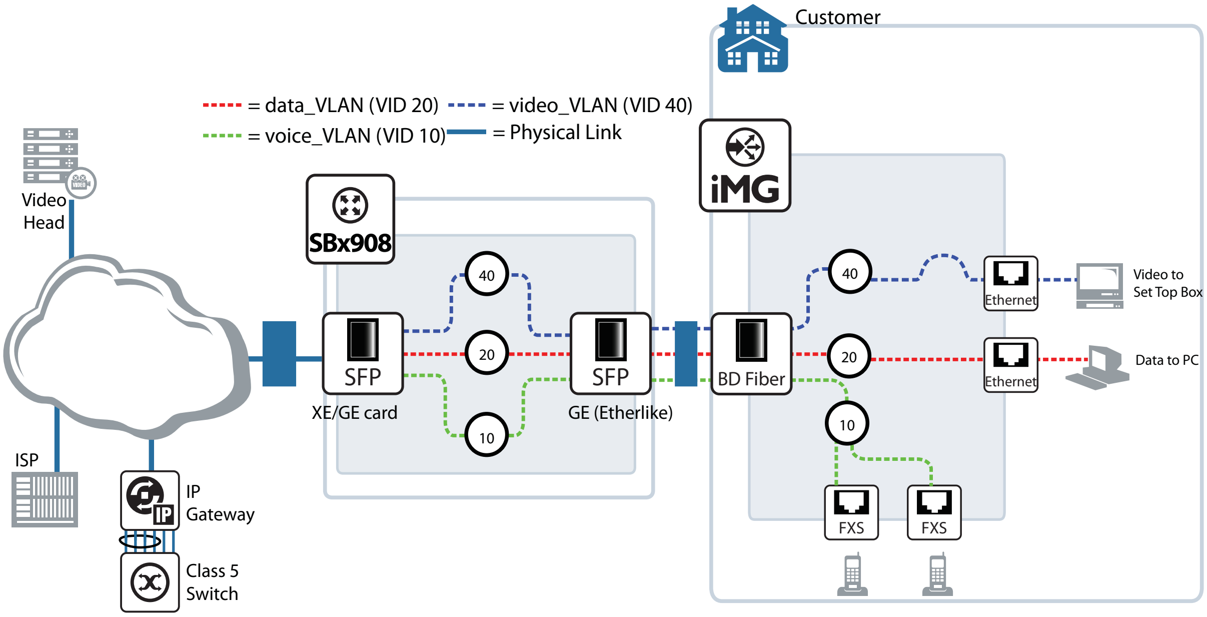
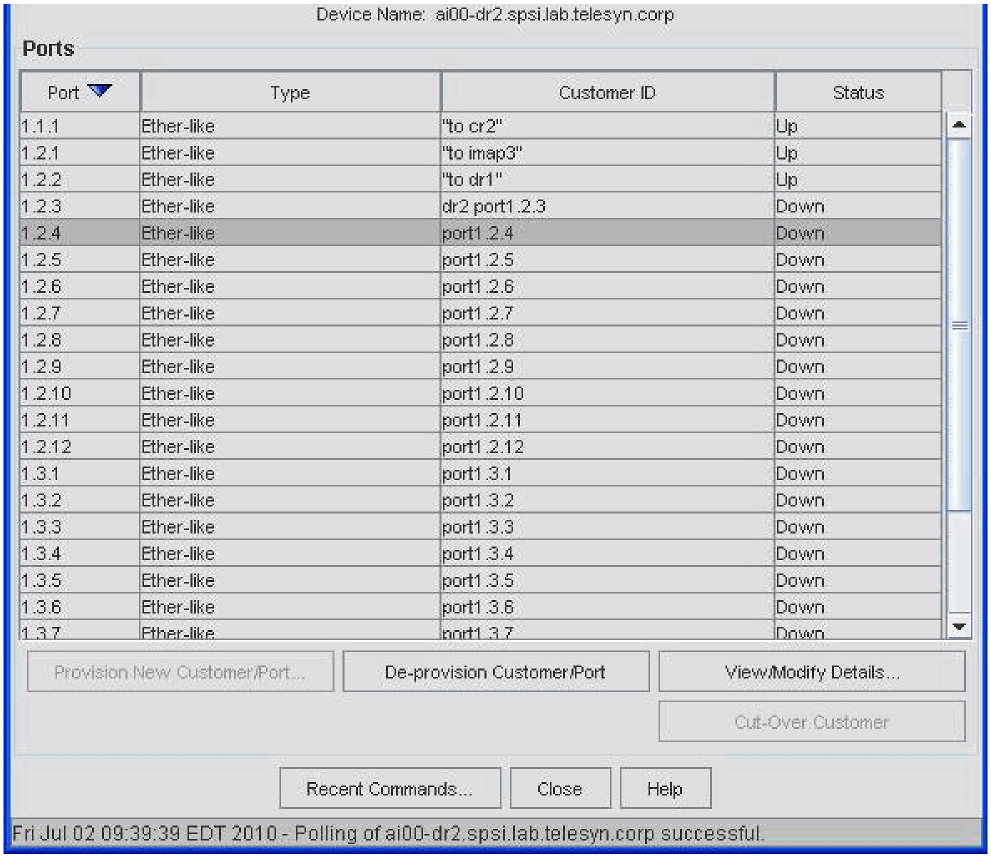


FIGURE 24-31 iMG/RG Connected to x908 Upstream Device.

The Triple-Play form can be used to pre-provision the iMG/RG using the already created Profiles. The Triple-Play form is filled out as with other upstream devices, as shown Figure 24-33.

The few points to note in configuring iMG/RGs to AlliedWare Plus devices are:

- When an AW+ product is first installed, you must use the NMS to deprovision the ports before provisioning the ports. This is because they have default descriptions (CustomerID) such as port1.2.4, as shown in the following figure.



Device Name: ai00-dr2.spsi.lab.telesyn.corp

Ports

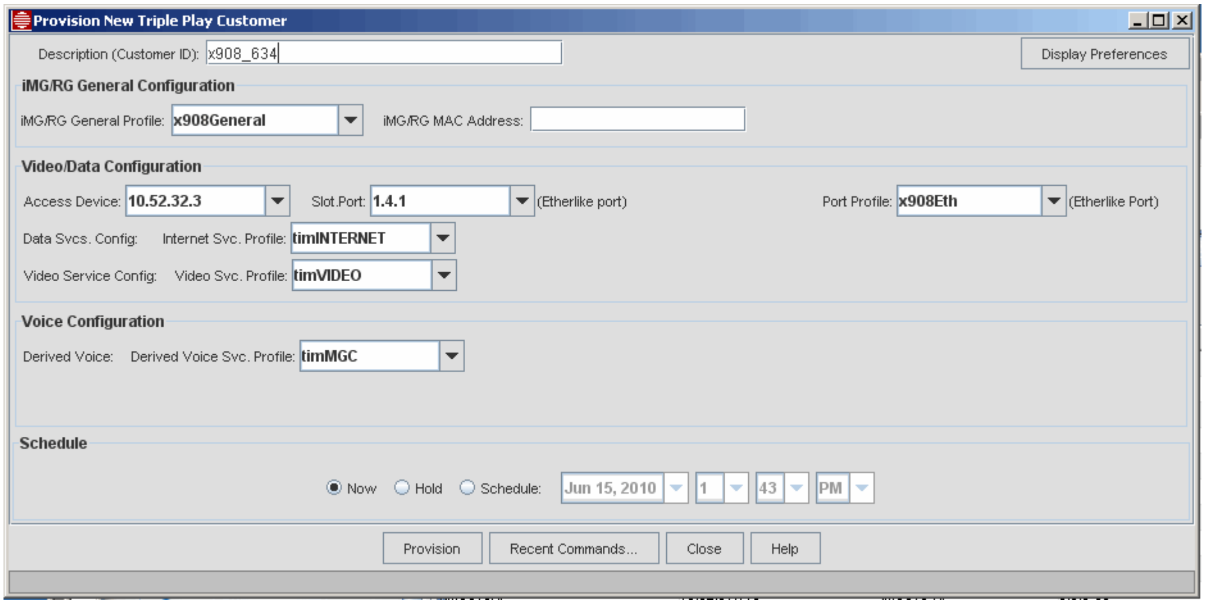
Port	Type	Customer ID	Status
1.1.1	Ether-like	"to cr2"	Up
1.2.1	Ether-like	"to imap3"	Up
1.2.2	Ether-like	"to dr1"	Up
1.2.3	Ether-like	dr2 port1.2.3	Down
1.2.4	Ether-like	port1.2.4	Down
1.2.5	Ether-like	port1.2.5	Down
1.2.6	Ether-like	port1.2.6	Down
1.2.7	Ether-like	port1.2.7	Down
1.2.8	Ether-like	port1.2.8	Down
1.2.9	Ether-like	port1.2.9	Down
1.2.10	Ether-like	port1.2.10	Down
1.2.11	Ether-like	port1.2.11	Down
1.2.12	Ether-like	port1.2.12	Down
1.3.1	Ether-like	port1.3.1	Down
1.3.2	Ether-like	port1.3.2	Down
1.3.3	Ether-like	port1.3.3	Down
1.3.4	Ether-like	port1.3.4	Down
1.3.5	Ether-like	port1.3.5	Down
1.3.6	Ether-like	port1.3.6	Down
1.3.7	Ether-like	port1.3.7	Down

Fri Jul 02 09:39:39 EDT 2010 - Polling of ai00-dr2.spsi.lab.telesyn.corp successful.

FIGURE 24-32 Provisioning Ports on AlliedWare Plus Devices

Note: After the ports have been provisioned with the NMS, then de-provisioned, their customer ids remain blank. Over time all non-provisioned ports will be blank. It's only when the device is newly installed that they have default descriptions and require this extra de-provisioning step.

- Upstream port numbering - These use the 3-number format (for stack.module.port)
- Each AlliedWare Plus device must function as an L3 Router.
- Customers on each switch must be in non-shared subnets, because these AlliedWare Plus devices do standard DHCP Relay with option 82 as circuit ID only (no remote ID) and do not perform DHCP Snooping.



Description (Customer ID): x908_634

iMG/RG General Configuration

iMG/RG General Profile: x908General

iMG/RG MAC Address:

Video/Data Configuration

Access Device: 10.52.32.3

Slot.Port: 1.4.1 (Etherlike port)

Port Profile: x908Eth (Etherlike Port)

Data Svcs. Config: Internet Svc. Profile: timINTERNET

Video Service Config: Video Svc. Profile: timVIDEO

Voice Configuration

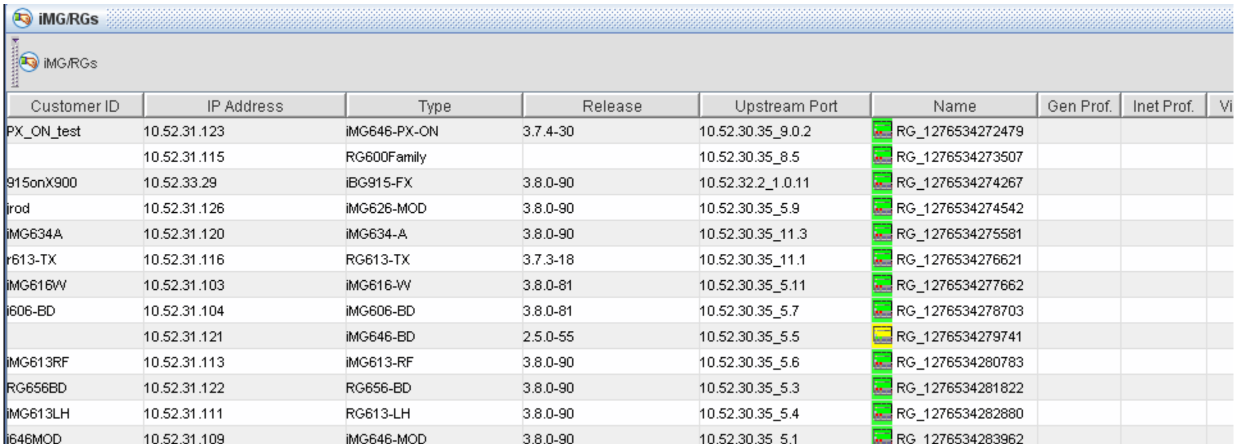
Derived Voice: Derived Voice Svc. Profile: timMGC

Schedule

● Now ○ Hold ○ Schedule: Jun 15, 2010 1 43 PM

FIGURE 24-33 Triple Play Form with x908 Upstream Device

Once the form is filled in and the NMS has performed provisioning in software, the iMG will begin its provisioning either immediately (if the iMG/RG is already connected and powered on), or later (when the iMG /RG is connected and powered on). When complete, the iMG is listed and includes its IP address, upstream port, and the associated profiles. Refer to the following figure.



Customer ID	IP Address	Type	Release	Upstream Port	Name	Gen Prof.	Inet Prof.	Vi
PX_ON_test	10.52.31.123	iMG646-PX-ON	3.7.4-30	10.52.30.35_9.0.2	RG_1276534272479			
	10.52.31.115	RG600Family		10.52.30.35_8.5	RG_1276534273507			
915onX900	10.52.33.29	iBG915-FX	3.8.0-90	10.52.32.2_1.0.11	RG_1276534274267			
jrod	10.52.31.126	iMG626-MOD	3.8.0-90	10.52.30.35_5.9	RG_1276534274542			
iMG634A	10.52.31.120	iMG634-A	3.8.0-90	10.52.30.35_11.3	RG_1276534275581			
r613-TX	10.52.31.116	RG613-TX	3.7.3-18	10.52.30.35_11.1	RG_1276534276621			
iMG616W	10.52.31.103	iMG616-W	3.8.0-81	10.52.30.35_5.11	RG_1276534277662			
i606-BD	10.52.31.104	iMG606-BD	3.8.0-81	10.52.30.35_5.7	RG_1276534278703			
	10.52.31.121	iMG646-BD	2.5.0-55	10.52.30.35_5.5	RG_1276534279741			
iMG613RF	10.52.31.113	iMG613-RF	3.8.0-90	10.52.30.35_5.6	RG_1276534280783			
RG656BD	10.52.31.122	RG656-BD	3.8.0-90	10.52.30.35_5.3	RG_1276534281822			
iMG613LH	10.52.31.111	RG613-LH	3.8.0-90	10.52.30.35_5.4	RG_1276534282880			
i646MOD	10.52.31.109	iMG646-MOD	3.8.0-90	10.52.30.35_5.1	RG_1276534283962			

FIGURE 24-34 iMG/RG Provisioned - Complete

24.9 Configuration 9 - Microsoft Mediaroom with the iMG/RG

The Mediaroom configuration is sometimes referred to as a “whole home” configuration. With Mediaroom you can configure the iMG/RG device to allow all devices that are connected to the iMG to communicate to each other and share content. In this configuration all Mediaroom devices such as PCs, printers, DVRs, STBs, etc. can share content through the same local network. (Additional configuration may be required in STB, PC or other Mediaroom devices to setup a fully connected Mediaroom environment.)

Sharing a local network also allows you to connect any video or data devices to LAN ports configured for Mediaroom with the iMG. The iMG assigns IP addresses to connected devices using DHCP and allows data sharing through the local network with connections to upstream services as requested by Mediaroom devices.

Examples where this type of communication is useful include:

- Sharing a networked printer in a home where there are multiple PCs
- Recording TV broadcast to a DVR and viewing on demand content from the DVR to a PC or STB
- Viewing video, pictures and music libraries stored in a PC on a TV
- Future applications may also include networked appliances (e.g. smart refrigerator, etc.)

The iMG/RG can support three configurations:

1. Separate upstream VLANs - This model uses a separate upstream VLAN for each service and also requires a separate management VLAN. This is a model already supported by the NMS.
2. Single upstream VLAN with multiple virtual IP interfaces - This model uses one upstream VLAN and separate virtual interfaces for management, data and voice. A single VLAN simplifies WAN VLAN setup but adds configuration for new virtual interfaces (Virtual interface configuration support is new in iMGs 3-8).
3. Single upstream VLAN with a single IP interface - This model uses a single upstream VLAN and also a single IP address for the iMG. Network configuration is simplified using one VLAN for all services but is less secure because video, data (Internet) and management traffic are using the same VLAN.

The NMS initially supports Model 1, which is already supported by the NMS. Therefore, the overall steps do not change, but there are additions to the profiles to provision the iMG.

Figure 24-35 shows the basic configuration.

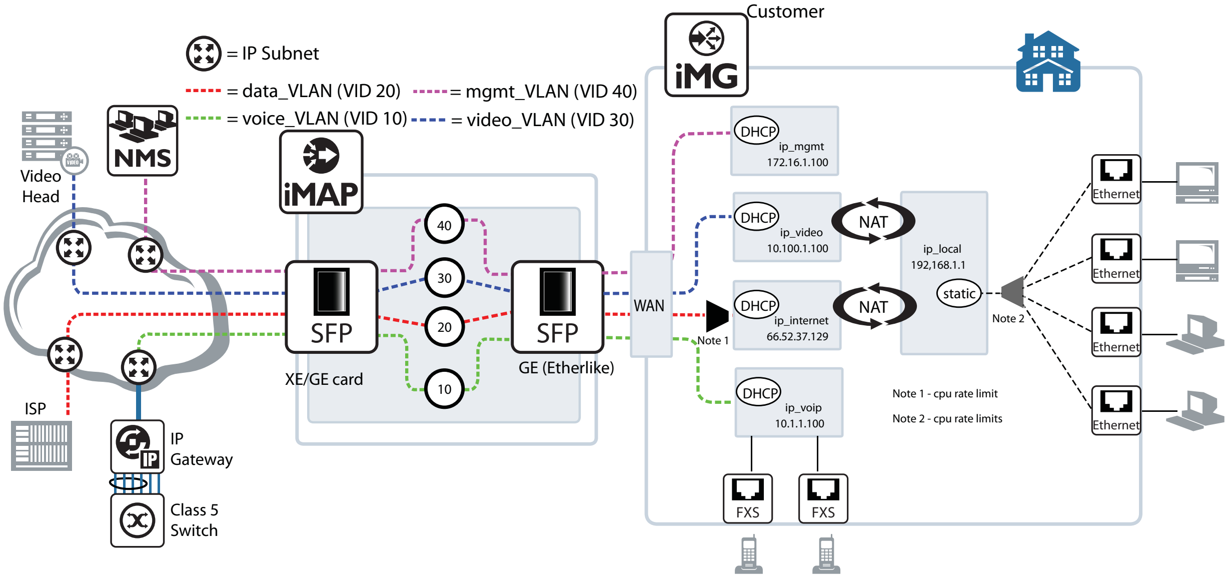


FIGURE 24-35 Mediaroom Configuration

The figure shows the separate upstream VLANs model to support the Mediaroom configuration with the iMG. On the upstream side the VLANs follow the existing model, but on the iMG all LAN ports used for Mediaroom are added to the local VLAN, with the local network shared with multiple NAT instances that route local traffic to the VLANs configured to provide service to the connected Mediaroom device. In this model the management and voice VLANs are unchanged because these are not attached to LAN ports. All data and video traffic is routed at the CPE from the local VLAN to upstream VLAN (no bridged Internet), and the local VLAN is configured to assign IP addresses to all media devices using DHCP.

Several configuration fields are required for Mediaroom functionality. These fields are part of the General, Internet and Video profiles.

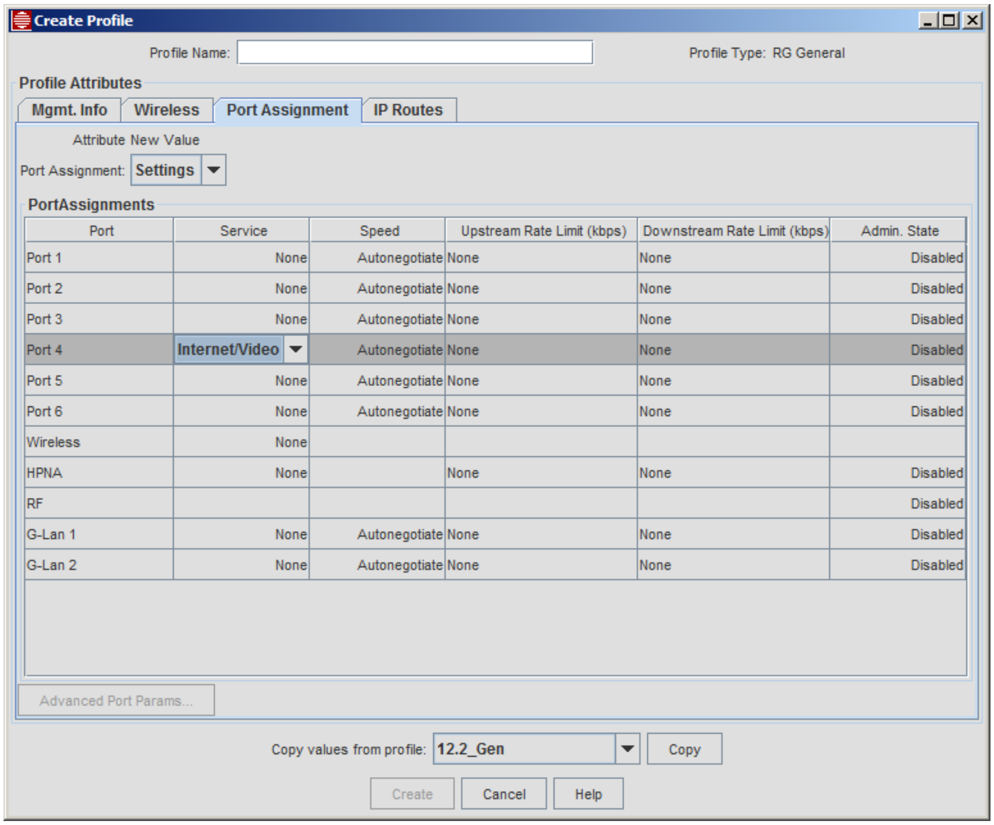
Mediaroom configuration differs depending on the type of device you are configuring. Some of the fields utilized by the iMG 600, iMG 700, and iBG 910 series devices do not apply to the iMG 1000 and iMG 2000 series devices.

24.9.1 iMG/RG General Profile

In a Mediaroom configuration you can connect local media devices to any non-wireless port to receive service. The ports must be configured as an **Internet/Video** service to indicate they can receive either video or data traffic. The **Internet/Video** service also applies to the services available on HPNA ports.

1. Create or modify an iMG/RG General Profile. Select the **Port Assignment** tab.
2. In the **Service** column, select **Internet/Video** for the Mediaroom ports.

- If you are configuring an iMG 1000 or iMG 2000 series device, all Internet ports must be set to **Internet/Video**. When one port is set to **Internet/Video** the rest of the Internet ports will automatically be set to **Internet/Video** as well.



Profile Name:

Profile Type: RG General

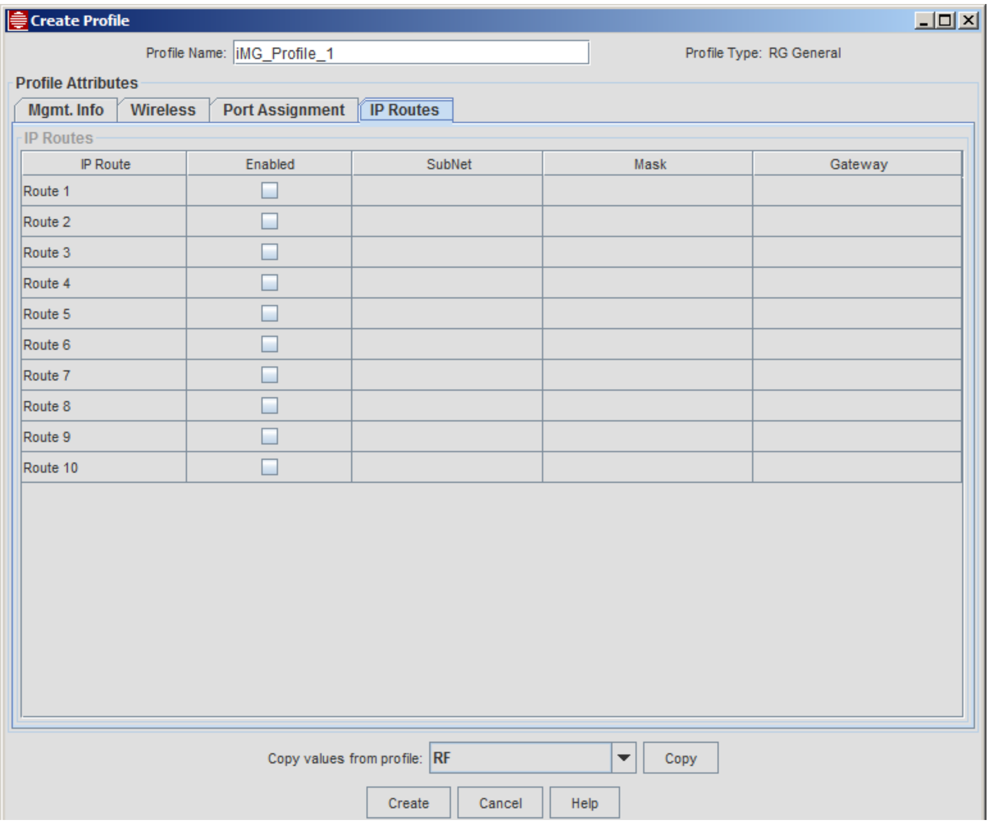
Port Assignment: Settings

Port	Service	Speed	Upstream Rate Limit (kbps)	Downstream Rate Limit (kbps)	Admin. State
Port 1	None	Autonegotiate	None	None	Disabled
Port 2	None	Autonegotiate	None	None	Disabled
Port 3	None	Autonegotiate	None	None	Disabled
Port 4	Internet/Video	Autonegotiate	None	None	Disabled
Port 5	None	Autonegotiate	None	None	Disabled
Port 6	None	Autonegotiate	None	None	Disabled
Wireless	None				
HPNA	None		None	None	Disabled
RF					Disabled
G-Lan 1	None	Autonegotiate	None	None	Disabled
G-Lan 2	None	Autonegotiate	None	None	Disabled

Copy values from profile: 12.2_Gen

FIGURE 24-36 Port Configuration for Mediaroom - Internet/Video Service

3. Select the **IP Routes** tab. The routes table allows up to 10 different routes in the iMG. Mediaroom devices connected to the iMG may request services configured in separate subnets on the upstream network.



Profile Name: iMG_Profile_1

Profile Type: RG General

IP Route	Enabled	SubNet	Mask	Gateway
Route 1	☐			
Route 2	☐			
Route 3	☐			
Route 4	☐			
Route 5	☐			
Route 6	☐			
Route 7	☐			
Route 8	☐			
Route 9	☐			
Route 10	☐			

Copy values from profile: RF

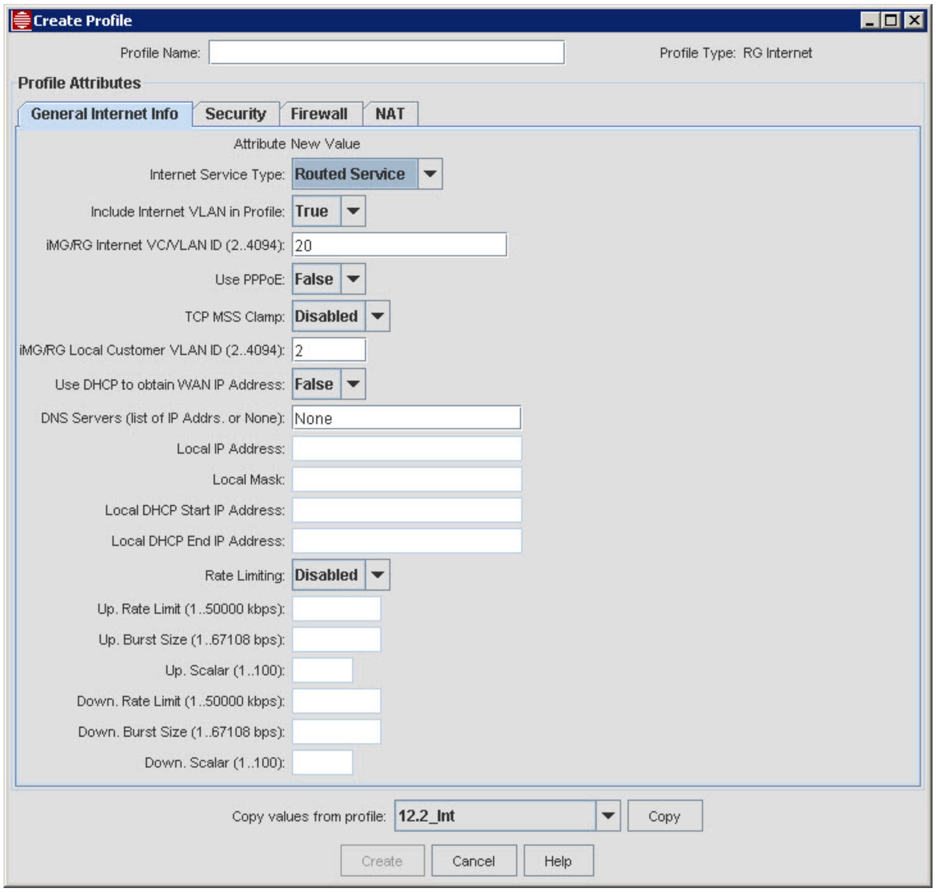
FIGURE 24-37 IP Routes for Mediaroom - Routes

4. If you are creating a new profile, ensure the entire profile is complete and click **Create**. If you are modifying an existing profile, click **Modify**.

24.9.2 iMG/RG Internet Profile

Note: Several fields in the Internet Profile are dependent on each other; that is, some fields are not available until other fields are set. Make sure to follow the steps below in the order given to ensure the fields you need to set are available.

1. Create or modify an iMG/RG Internet Profile. Select the **General Internet Info** tab.
2. In the **Internet Service Type** drop-down list, select **Routed Service**.



Profile Name:

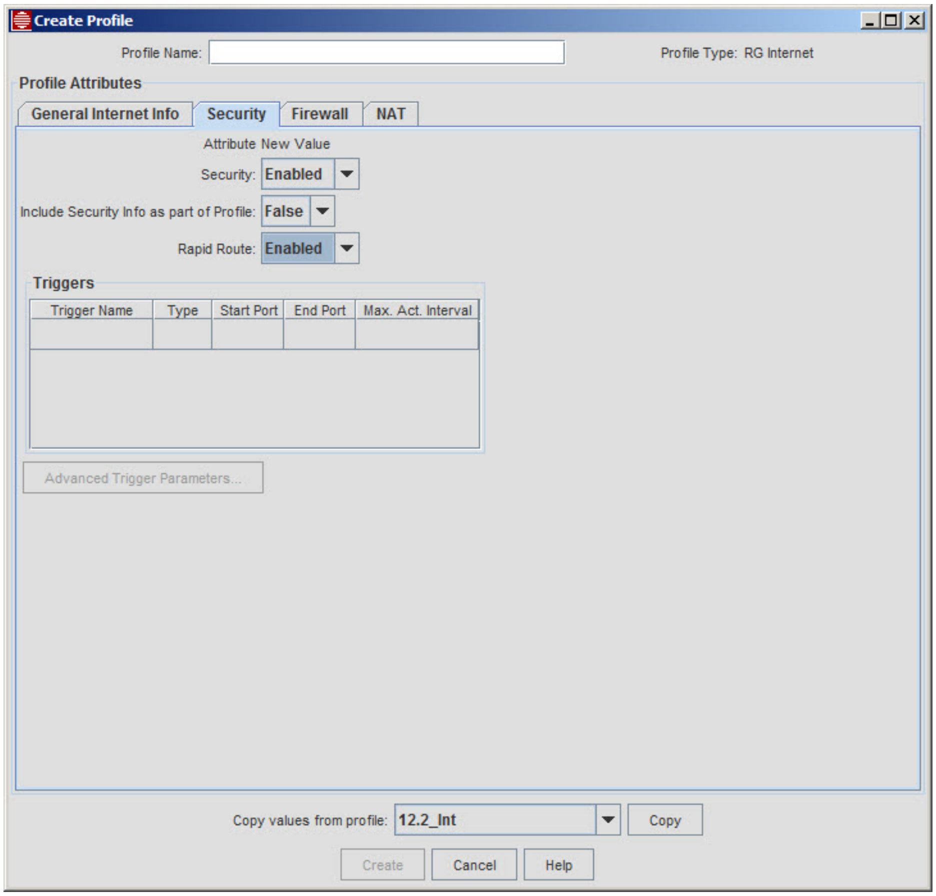
Profile Type: RG Internet

Attribute	New Value
Internet Service Type:	Routed Service
Include Internet VLAN in Profile:	True
iMG/RG Internet VC/VLAN ID (2..4094):	20
Use PPPoE:	False
TCP MSS Clamp:	Disabled
iMG/RG Local Customer VLAN ID (2..4094):	2
Use DHCP to obtain WAN IP Address:	False
DNS Servers (list of IP Addrs. or None):	None
Local IP Address:	
Local Mask:	
Local DHCP Start IP Address:	
Local DHCP End IP Address:	
Rate Limiting:	Disabled
Up. Rate Limit (1..50000 kbps):	
Up. Burst Size (1..67108 bps):	
Up. Scalar (1..100):	
Down. Rate Limit (1..50000 kbps):	
Down. Burst Size (1..67108 bps):	
Down. Scalar (1..100):	

Copy values from profile: 12.2_Int

FIGURE 24-38 Internet Service Type for Mediaroom - Routed Service

3. Select the **Security** tab.
4. In the **Security** drop-down list, select **Enabled**. Security must be enabled before you can complete subsequent steps.
5. If you are configuring an iMG 600, iMG 700, or iBG 910 series device, in the **Rapid Route** drop-down list, select **Enabled**. This enhances NAT routing functionality in the iMG for better throughput of routed traffic.



Create Profile

Profile Name:

Profile Type: RG Internet

Profile Attributes

Attribute	New Value
Security:	Enabled
Include Security Info as part of Profile:	False
Rapid Route:	Enabled

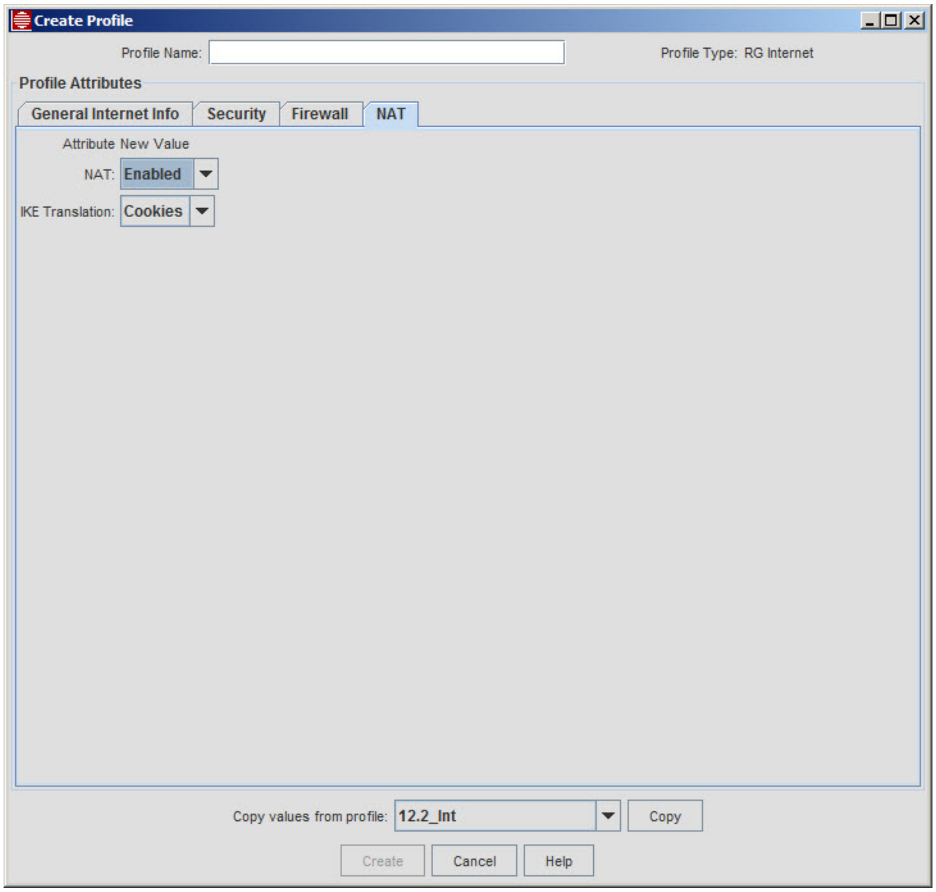
Triggers

Trigger Name	Type	Start Port	End Port	Max. Act. Interval

Copy values from profile: 12.2_Int

FIGURE 24-39 Security and Rapid Route for Mediaroom

6. Select the **NAT** tab.
7. In the **NAT** drop-down list, select **Enabled**. NAT must be enabled before you can set the address fields on the **General Internet Info** tab.



Profile Name:

Profile Type: RG Internet

Profile Attributes

Attribute New Value

NAT: Enabled

IKE Translation: Cookies

Copy values from profile: 12.2_Int

FIGURE 24-40 NAT for Mediaroom

8. Select the **General Internet Info** tab. You can now set the following fields:

   Local IP Address

   Local Mask

   Local DHCP Start IP Address

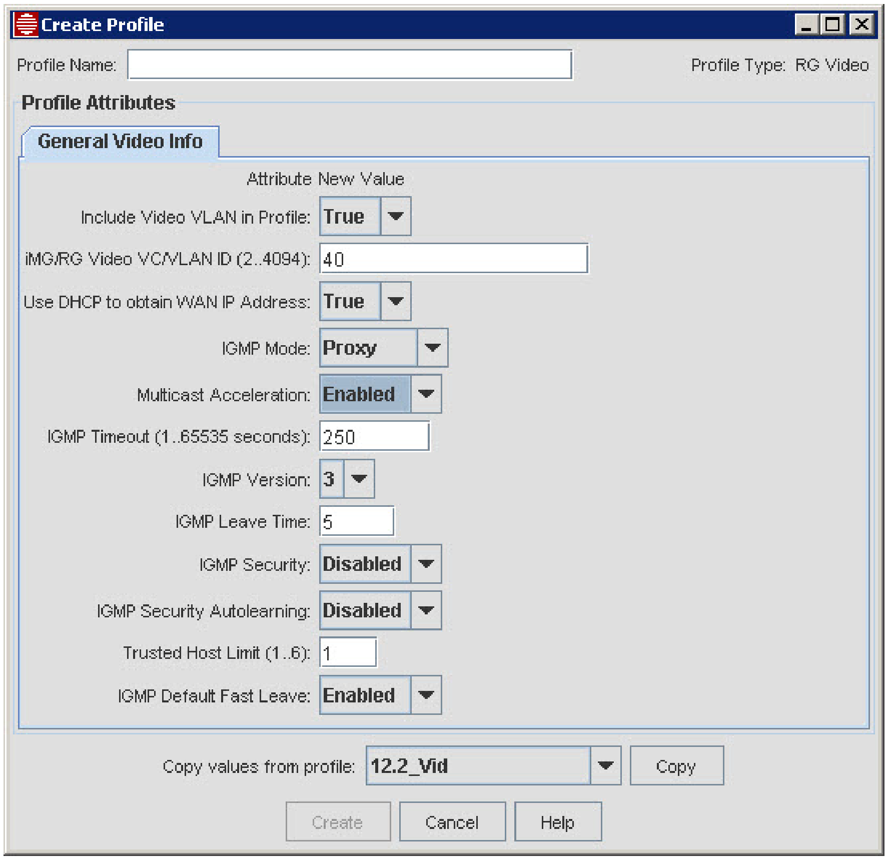
   Local DHCP End IP Address

9. If you are creating a new profile, ensure the entire profile is complete and click **Create**. If you are modifying an existing profile, click **Modify**.

24.9.3 iMG/RG Video Profile

Since Mediaroom services are routed, the Video profile allows obtaining the IP address for video service using DHCP since this must be a valid reachable IP address. The IP addresses for the video interface can also be set in the Triple Play Provision window, or after provisioning using the View/Modify Details window.

1. Create or modify an iMG/RG Video Profile.
2. In the **IGMP Mode** drop-down list, select **Proxy**. This must be set first in order to set the **Use DHCP to obtain WAN IP Address** field.
3. In the **Use DHCP to obtain WAN IP Address** drop-down list, select **True**.
4. If you are configuring an iMG 600, iMG 700, or iBG 910 series device, in the **Multicast Acceleration** drop-down list, select **Enabled**. This will configure the upstream VLAN so that multicast traffic can travel across the local VLAN and the upstream video VLAN.



Profile Name:

Profile Type: RG Video

Attribute	New Value
Include Video VLAN in Profile:	True
iMG/RG Video VC/VLAN ID (2..4094):	40
Use DHCP to obtain WAN IP Address:	True
IGMP Mode:	Proxy
Multicast Acceleration:	Enabled
IGMP Timeout (1..65535 seconds):	250
IGMP Version:	3
IGMP Leave Time:	5
IGMP Security:	Disabled
IGMP Security Autolearning:	Disabled
Trusted Host Limit (1..6):	1
IGMP Default Fast Leave:	Enabled

Copy values from profile: 12.2_Vid

FIGURE 24-41 iMG/RG Video Profile for Mediaroom

5. If you are creating a new profile, ensure the entire profile is complete and click **Create**. If you are modifying an existing profile, click **Modify**.

After configuring the profiles, you provision the iMG device using the Triple Play form. Profiles are included as with other configurations.

24.9.3.1 Mediaroom Device Support

For iMG 600, iMG 700, and iBG 910 series devices, Mediaroom features are available only for those that support iMG 3-8 and above. If Mediaroom profiles are used on devices that do not support the functionality the configuration is not applied and the LAN ports are configured for routed Internet service.

The following iMG 600 series devices do not support Mediaroom functionality:

- RG613-TX/TXJ/BD/SH/LH
- RG623-TX/BD/SH/LH
- iMG613-RF
- iMG616-BD/SH/LH/RF/RF+/SRF+
- iMG624-A/B
- iMG634-A/B
- iMG634-WA/WB

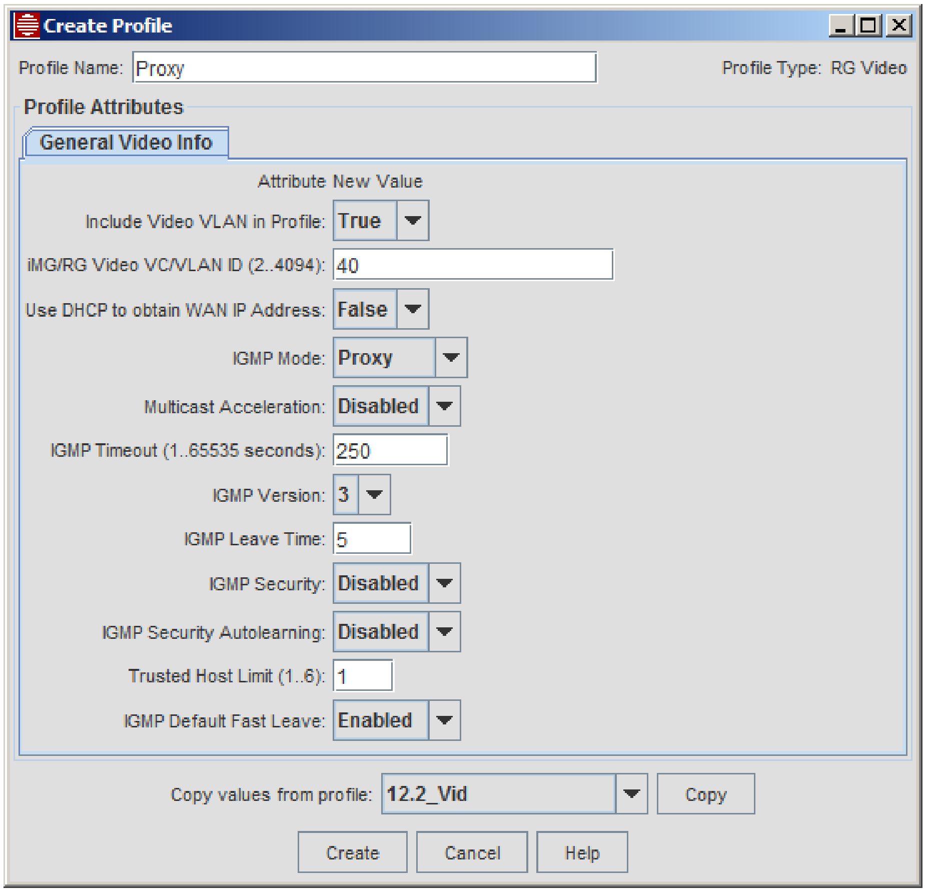
24.10 Configuration 10 - Video with static IP Address (iMG 1000 and iMG 2000 Series)

In most networks, for security reasons routers will not accept source IP addresses of all zeros or will ensure that the IGMP traffic (including joins/leaves) has a proper IP address. When setting up video service, you can set the IGMP Mode to Proxy, but must then either:

- Set the “Use DHCP to obtain WAN IP Address” to True
- Set the “Use DHCP to obtain WAN IP Address” to False and include a static IP address and mask.

Note: For iMGs with 3-8 loads, the IP address used is the iMG Mgmt IP.

Refer to the following figure for the Video Profile attributes.



Profile Name: Proxy

Profile Type: RG Video

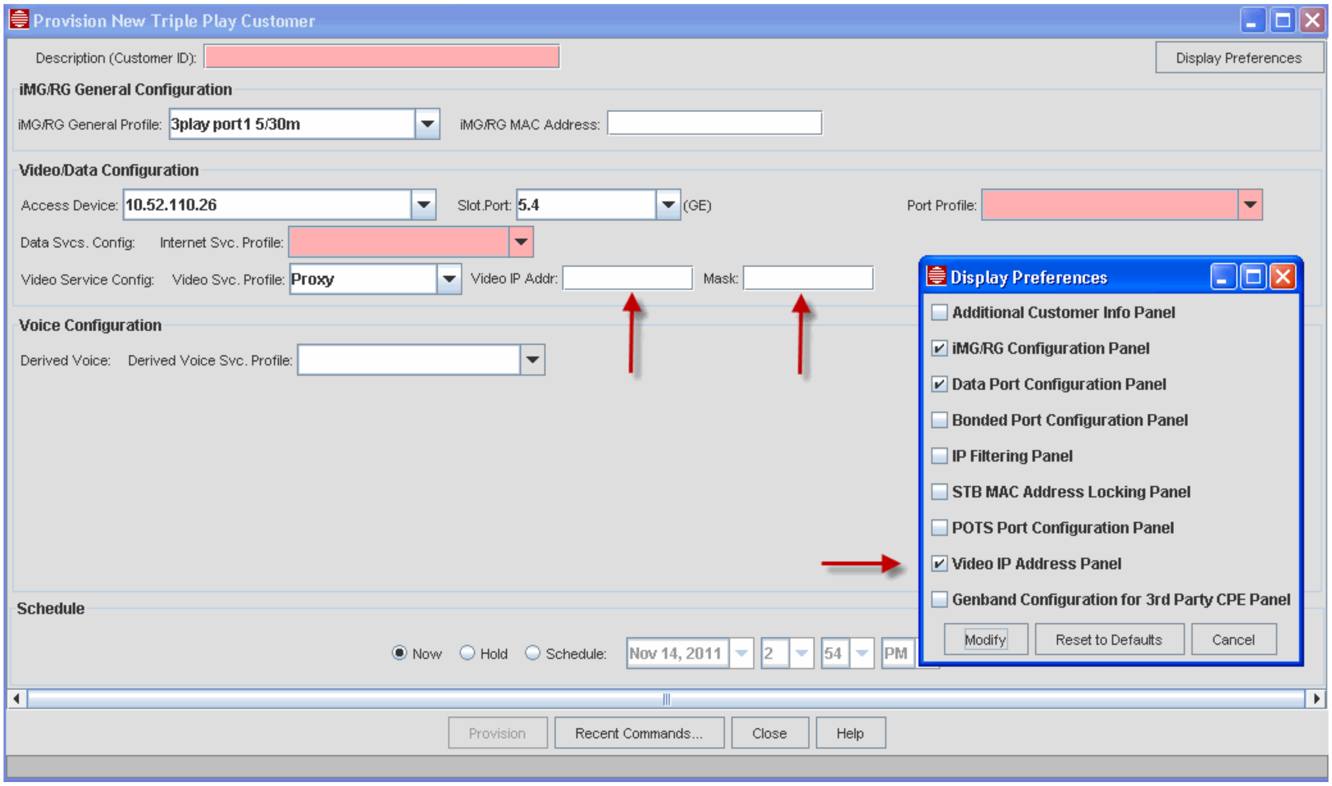
Profile Attributes

Attribute	New Value
Include Video VLAN in Profile:	True
iMG/RG Video VC/VLAN ID (2..4094):	40
Use DHCP to obtain WAN IP Address:	False
IGMP Mode:	Proxy
Multicast Acceleration:	Disabled
IGMP Timeout (1..65535 seconds):	250
IGMP Version:	3
IGMP Leave Time:	5
IGMP Security:	Disabled
IGMP Security Autolearning:	Disabled
Trusted Host Limit (1..6):	1
IGMP Default Fast Leave:	Enabled

Copy values from profile: 12.2_Vid

FIGURE 24-42 Video Profile for Proxy Mode (Use DHCP Option = False)

When filling out the Triple-Play form, the administrator should select Display Preferences and select the tic-box VideoIP Address Panel. The user can then fill in a static Video IP Address and Mask, which allows video to work. Refer to the following figure.



Provision New Triple Play Customer

Description (Customer ID):

Display Preferences

iMG/RG General Configuration

iMG/RG General Profile: 3play port1 5/30m

iMG/RG MAC Address:

Video/Data Configuration

Access Device: 10.52.110.26

Slot.Port: 5.4 (GE)

Port Profile:

Data Svcs. Config: Internet Svc. Profile:

Video Service Config: Video Svc. Profile: Proxy

Video IP Addr:

Mask:

Voice Configuration

Derived Voice: Derived Voice Svc. Profile:

Schedule

● Now ○ Hold ○ Schedule: Nov 14, 2011 2 54 PM

Display Preferences

□ Additional Customer Info Panel

☑ iMG/RG Configuration Panel

☑ Data Port Configuration Panel

□ Bonded Port Configuration Panel

□ IP Filtering Panel

□ STB MAC Address Locking Panel

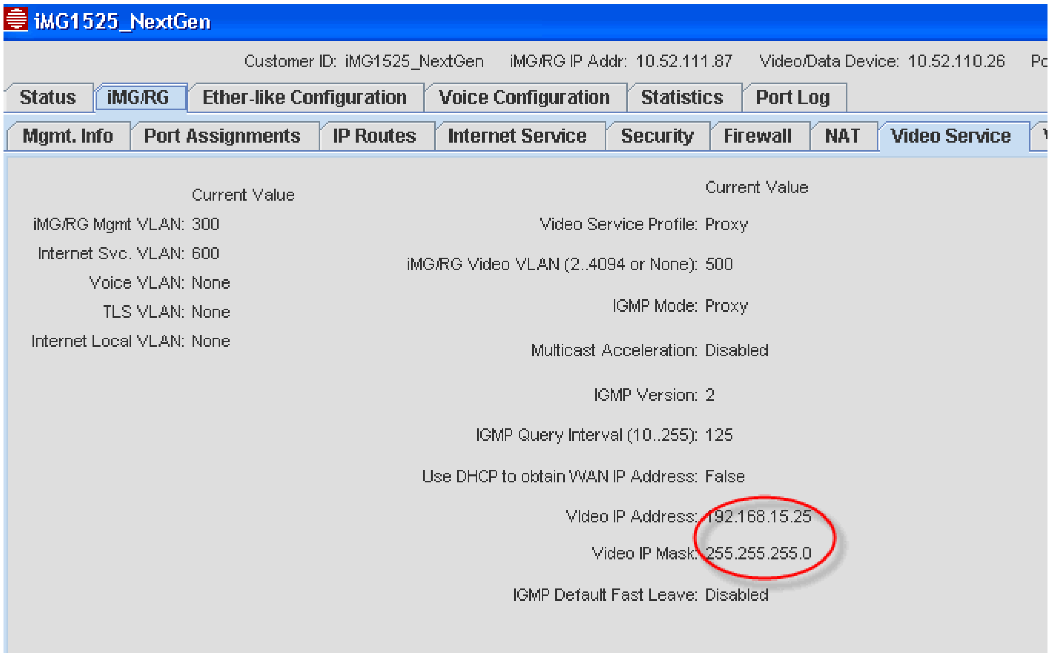
□ POTS Port Configuration Panel

☑ Video IP Address Panel

□ Genband Configuration for 3rd Party CPE Panel

FIGURE 24-43 Showing the Video IP Address Panel (Display Preferences Option)

Once configured, the *iMG/RG -> Video Service* tab shows the Video IP Address and Video IP Mask, as shown below.



iMG1525_NextGen

Customer ID: iMG1525_NextGen iMG/RG IP Addr: 10.52.111.87 Video/Data Device: 10.52.110.26 Po

Current Value

iMG/RG Mgmt VLAN: 300

Internet Svc. VLAN: 600

Voice VLAN: None

TLS VLAN: None

Internet Local VLAN: None

Current Value

Video Service Profile: Proxy

iMG/RG Video VLAN (2..4094 or None): 500

IGMP Mode: Proxy

Multicast Acceleration: Disabled

IGMP Version: 2

IGMP Query Interval (10..255): 125

Use DHCP to obtain WAN IP Address: False

Video IP Address: 192.168.15.25

Video IP Mask: 255.255.255.0

IGMP Default Fast Leave: Disabled

FIGURE 24-44 Configure iMG with Static Video IP Address

25. Using the Performance View

Performance monitoring collects useful data from network devices and determining how efficiently the network is functioning. Performance is measured based on various factors, such as:

- The number of bytes of data received (over a period) by a particular interface of a device
- The number of bytes of data sent (over a period) by a particular interface of a device
- An estimate of the interface's current bandwidth in bits per second

The data pertaining to a network device are collected based on the definition of performance variables (otherwise called statistics and polled data).

Use the following table to locate the task you wish to perform. If you are using AlliedView NMS, use the screen name or form name as well to locate the relevant section.

TABLE 25-1 Task List for Performance Monitoring

Task	Screen / Form Name (if Applicable)	Section
Review Screen Components	Configured Collection	("Screen Components for Statistics" on page 967)
View Graphs	Not applicable (n/a)	("Viewing a Graph" on page 969)
Print a Graph	n/a	("Printing a Graph" on page 970)
View Data Real Time	n/a	("Viewing Real Time Data" on page 970)
Configure Thresholds	Threshold Properties	("Overview" on page 972)
Configure Statistics	Data Collection Detailed Properties	("Configuring Statistics" on page 973) (Administrator Task)

25.1 Polling Concepts

The process of collecting the data from a network device is called *polling*. Every statistic has the following details:

- The data to poll
- The device from which the data will be polled
- The polling interval

The following figure lists the basic flow for Performance Monitoring.

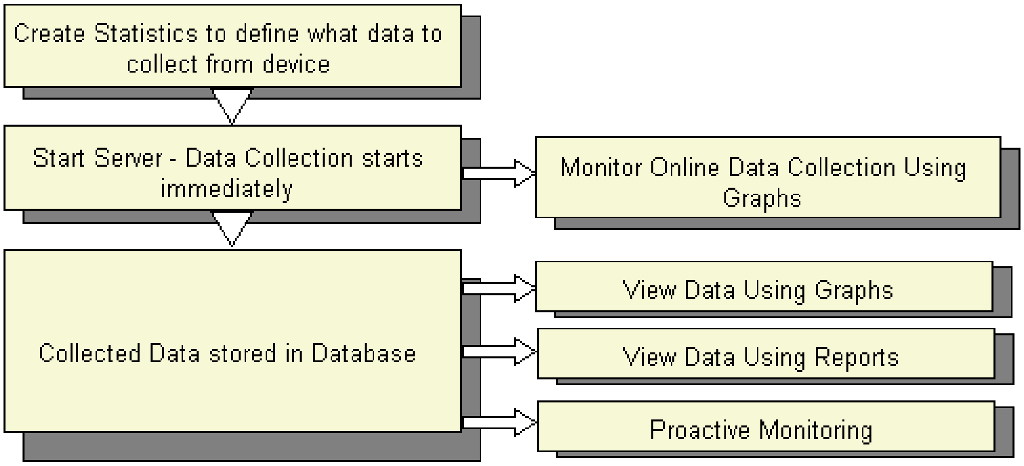

Create Statistics to define what data to collect from device
Start Server - Data Collection starts immediately
Monitor Online Data Collection Using Graphs
Collected Data stored in Database
View Data Using Graphs
View Data Using Reports
Proactive Monitoring

FIGURE 25-1 Setting up Performance Monitoring

The person or persons responsible for performance monitoring will have the following tasks, which are explained in detail later in this section:

- Viewing Data Collection Details - Statistics are the basic unit of network data collection. The data about a network device is collected based on the definition of a statistic.
- Creating a Custom View - By default, you are able to view all the statistics of all the network devices in the Configured Collection panel. To view very often a particular set of statistics you can create a custom view and specify the matching criteria. Only those statistics that match the specified condition will appear in the custom view.
- Viewing the Data - AlliedView NMS allows you to plot collected statistical data as bar or line graphs. This is useful for trend analysis. You can view the collected data in the form of graphs and reports.
- Monitoring Real-Time Data Collection - If you want to view the data as it is collected rather than fetching it from the database, you can choose this option. This is otherwise called *on line data collection monitoring*. You may require this when you want to view the data currently collected for the device. Graphs and tables are available for monitoring.

25.2 Data Collection Interface

The interface for performance data in the AlliedView NMS is the Configured Collection view under the Performance node in the NMS Tree. This view displays the statistics for the nodes on the network and is used as the interface to the data.

25.2.1 Setting Up the Interface

Before starting any data collection process, you must define what data to poll, from where, in what interval, etc. This definition is created in objects called Statistics. To collect *n* type of data from a device you have to create *n* Statistics. The NMS Administrator can configure this setup and add more Statistics, if necessary, before the AlliedView NMS server starts. The NMS Administrator can also add Statistics at runtime. You can view the list of statistics associated with each of the MOs discovered in the network using the Configured Collection panel.

Note: An MO represents a network element for which data have to be collected. It can be a node, interface, a port, a card, a slot, etc.

25.2.2 Panel-Specific Menus for the Configured Collection View

When the Configured Collection view is displayed in the NMS Display Panel, the following items appear in the Panel-Specific Menu Bar that are specific to the Configured Collection view:

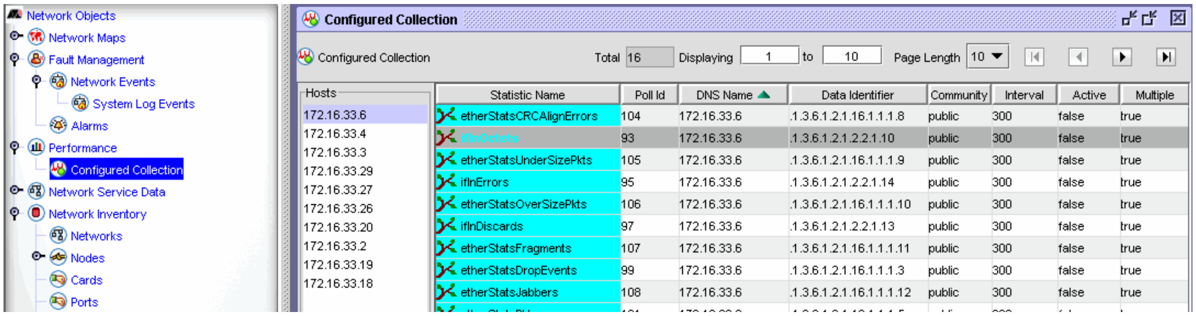
- *Edit* - Provides editing functions for the view. Items include:

  - *Threshold* - Provides the ability to add, modify, and delete thresholds.
  - *Polling Objects* - Provides the ability to view, add, modify, and delete polling objects.
  - *Add Statistic* - Provides the ability to add a new statistic.
  - *Remove Statistic* - Provides the ability to remove a statistic.
  - *Modify Statistic* - Provides the ability to modify a statistic.
  - *Search* - Provides a search function for the view (refer to "Searching in a View" on page 90).
  - *Export Table Data* - Provides an export function for all of the view data. The data may be exported to a file (in delimited tabular form) or to a Web browser. The data may also be filtered.
  - *Export Selected Rows* - Provides an export function for selected rows in the view data.
- *View* - Provides additional display functions for the view. The items include:
  - *Plot* - Provides graphing functions for the current and collected statistics. Refer to "Using Graphs" on page 969.
  - *Refresh* - Refreshes the view data.
- *Actions* - Provides a *Save To File* option, which saves the event information to a file.

25.2.3 Screen Components for Statistics

To access the Data Collection screen, perform the following:

1. Select the Configured Collection node from the tree in the left frame. You can see the Configured Collection panel in the right frame, which displays a list of nodes under the Hosts column. This list indicates that these devices have been identified in the network for data collection.
2. Select any of the hosts, and you will see the associated Statistic. (Each row of information is called a Statistic). Refer to the following figure.



Total 16 Displaying 1 to 10 Page Length 10

Hosts

172.16.33.6
172.16.33.4
172.16.33.3
172.16.33.29
172.16.33.27
172.16.33.26
172.16.33.20
172.16.33.2
172.16.33.19
172.16.33.18

Statistic Name	Poll Id	DNS Name ▲	Data Identifier	Community	Interval	Active	Multiple
etherStatsCRCAlignErrors	104	172.16.33.6	.1.3.6.1.2.1.16.1.1.1.8	public	300	false	true
ifInOctets	93	172.16.33.6	.1.3.6.1.2.1.2.2.1.10	public	300	false	true
etherStatsUnderSizePkts	105	172.16.33.6	.1.3.6.1.2.1.16.1.1.1.9	public	300	false	true
ifInErrors	95	172.16.33.6	.1.3.6.1.2.1.2.2.1.14	public	300	false	true
etherStatsOverSizePkts	106	172.16.33.6	.1.3.6.1.2.1.16.1.1.1.10	public	300	false	true
ifInDiscards	97	172.16.33.6	.1.3.6.1.2.1.2.2.1.13	public	300	false	true
etherStatsFragments	107	172.16.33.6	.1.3.6.1.2.1.16.1.1.1.11	public	300	false	true
etherStatsDropEvents	99	172.16.33.6	.1.3.6.1.2.1.16.1.1.1.3	public	300	false	true
etherStatsJabbers	108	172.16.33.6	.1.3.6.1.2.1.16.1.1.1.12	public	300	false	true

FIGURE 25-2 Collection View Panel

The following table lists the components in.the previous figure.

TABLE 25-2 Data Collection Screen Components

Component	Description for Data Collection Screen Components
Property Columns	You can see for every statistic that the associated properties are displayed in columns. For example, Statistic name, Poll ID, Data Identifier, DNS Name, interval etc. The Administrator decides which properties are to be displayed. Some of the properties are described below. Statistic Name - A string to identify the Statistic uniquely. This should be a meaningful name describing the Statistic Poll ID - A unique number associated with each Statistic for AlliedView NMS Performance module to identify the Statistic. Poll ID is automatically generated and hence no two Statistics will have the same Poll ID. DNS Name - This is the Host name (device name) with which this Statistic is associated Data Identifier - This is the Identification number of the device interface from which data about the device is to be collected. This Data Identifier is otherwise called as Object Identifier (OID), which is unique for every device. A list of possible OIDs for a device exists in the MIB definition of the device. Interval - This specifies when data should be collected for the Statistic. For example, the value 300 indicates that after every 300 seconds, data is collected.
Page Length	You can see a drop-down box labeled Page Length, which displays a number of hosts to be displayed per page. By default, it is set to 10. Hence, you can see 10 hosts displayed in the left panel of the Configured Collection frame.
From and To Range	There are two text boxes available labeled Displaying and To. You can set values in these and see the hosts list in that range. For example, If you set Displaying as 4 and To as 13, you will be able to view from Host 4 to Host 13. By default, the hosts are displayed in reverse alphabetical order.
Navigation Buttons	You can see four navigation buttons provided at the top right of the frame. They are Go to first page, Go to previous page, Go to next page and Go to Last page respectively. They will be enabled and disabled automatically based on your choice of page length and total number of hosts
Total	This text box cannot be edited, and it shows the total number of hosts available for data collection.

Note: *The green colored branch-like image adjacent to the Statistic name denotes the type of Statistic. Statistics are of three types: Node, Interface, and Multiple. The symbol with multiple branches denotes that the statistic is of type Multiple (one node and all associated interfaces).*

If no data are to be collected for a Statistic, the data are disabled temporarily by the Administrator. In such a case, you will see the Statistic row displayed in blue color. Once it is activated, the row color changes to green.

25.3 Viewing Historical Data

Once the AlliedView NMS server starts, data collection also starts automatically. Data is collected from the devices listed under the Hosts list in the Configured Collection panel. Data is collected only for those Statistics listed in the panel for each host.

The collected data is stored in a database maintained by the AlliedView NMS. Every day's data is stored in separate database tables. Every table has a name with the current date appended to the name in the form STATSDATAmm_dd_yyyy. (The mm and dd fields may be one or two digits.) A sample database table name is STATSDATA4_23_2002, which contains data collected on April 23, 2002.

You can deal with the collected data in various ways:

- Allow the data to be stored in the database for later viewing (for long-period trend analysis).
- View the Data in the form of a graph.
- View the Data in the form of a report.

25.3.1 Using Graphs

Two types of graphs are provided: line graphs and bar graphs. The graph is plotted by fetching the collected data already available in the database. No update is made in the graph as it is being viewed; that is, there is no dynamic plotting of the graph for the data collected from the device for that moment.

25.3.2 Viewing a Graph

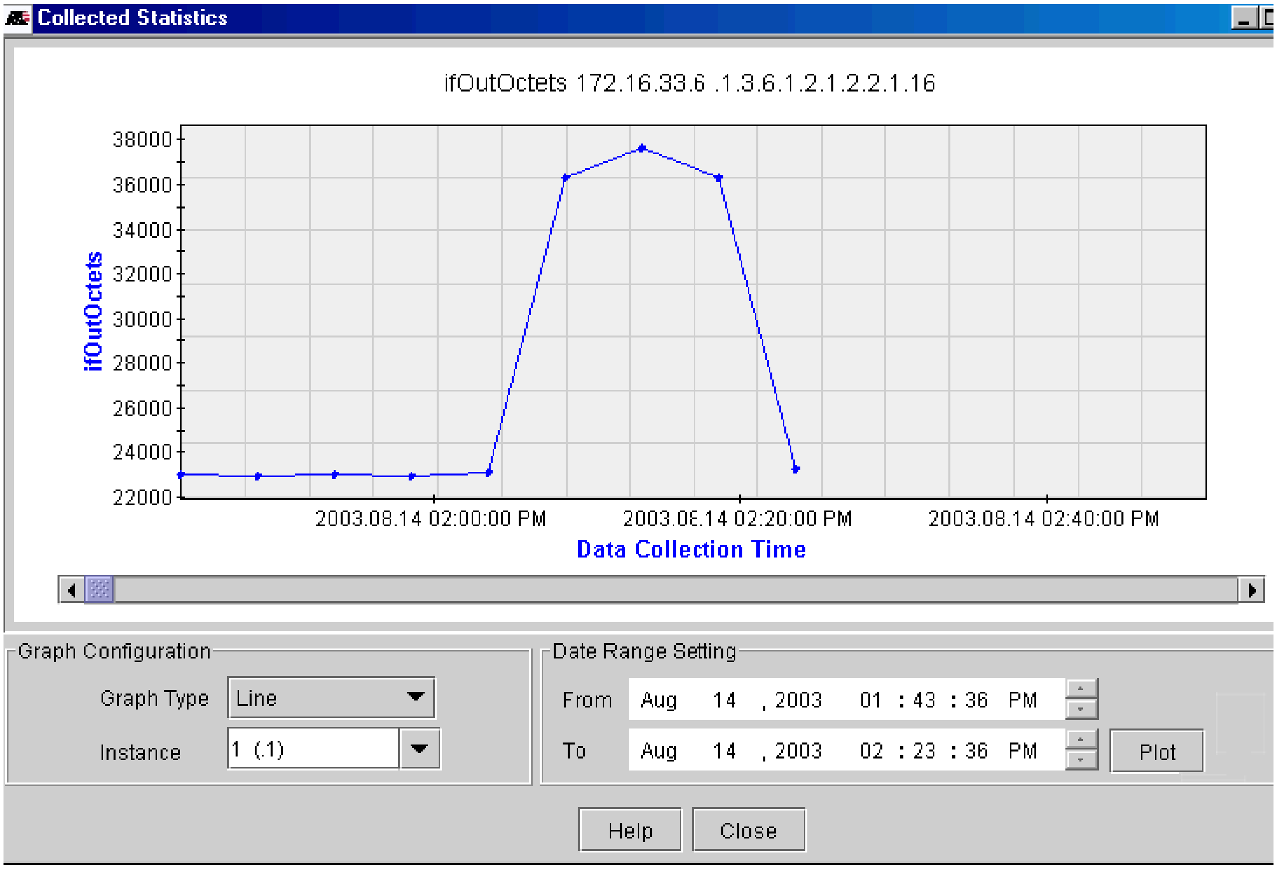
You can view the graph by following these steps:

1. Select the statistic in the Configured Collection panel for which you want to view the graph.
2. Select *View -> Plot -> Collected Statistic* from the Panel-Specific Menu Bar.

Possible Messages you may receive are:

- Data not yet Collected - By default, automatic data collection starts after five minutes after the server starts up. Also, data collection for a new statistic added via UI will start within five minutes of its creation. But this delay is configurable and will be set according to the requirement in your network. So do not get confused if you see the message **Data not yet collected** when you choose to view a graph or a report. It indicates that a data collection delay has been set. Please note that for counter-type OIDs, the first data collected is not stored. When second time data is collected, the difference between the two values is calculated and stored. Hence, depending on the polling interval set, the data will be collected on the second time. So, you might have more delay with respect to counter-type OIDs.
- A blank Graph and the message **No data collected** - There are two possible reasons:
    1. No data was collected for the current day, so choose Yes and change the From date and To date to view past data.
    2. The AlliedView NMS Server and Client are running on different machines and their time settings and time zones are not the same. Hence, synchronize the time settings to view the graph data.

The following figure shows the resulting graph.



Graph Configuration

Graph Type: Line

Instance: 1 (.1)

Date Range Setting

From: Aug 14, 2003 01 : 43 : 36 PM

To: Aug 14, 2003 02 : 23 : 36 PM

FIGURE 25-3 Collected Statistics Graph

Following are the main graph components:

- Graph Type - A drop-down box that displays two options, Line graph and Bar graph. You can choose any of these whenever you want and monitor the collected data.
- Data Range Setting - To view the data collected between a particular date range.
- **Plot** Button - Whenever you change the Graph type or Date Range, click the **Plot** button to restart plotting.

25.3.3 Printing a Graph

You can print the graph using the *Print* option provided in the Web browser or by using the Print Screen key on the keyboard.

25.3.4 Viewing Real Time Data

Once you narrow down your search and identify which device is the cause of the problem, you can use real-time monitoring to view and analyze the data of a particular statistic as it is collected from the device.

You cannot achieve this using Collected Statistics graph because of the following:

- The Collected Statistic graph displays only historical data; that is, past data available in the database.
- The Collected Statistic graph does not update its display when you are viewing it. Hence, to view the updates in the graph, you will have to either close the graph window and redisplay it periodically, or change the time range and then click the **Plot** button.

In this situation, you can select the current statistics graph.

Note: You might get an error message such as Time out, which indicates that the agent has been delayed in responding or the agent is down.

Assume, for steady performance, that you might need the value of the statistic ifInErrors to be between 13000 and 13500. You can monitor it in real time in this graph, and if the value goes beyond these limits, you can monitor it for another time period and decide on an appropriate action.

The Current Statistic graph (also referred to as a Runtime chart) provides two advantages when you do real-time monitoring:

1. You can change the Data Collection interval

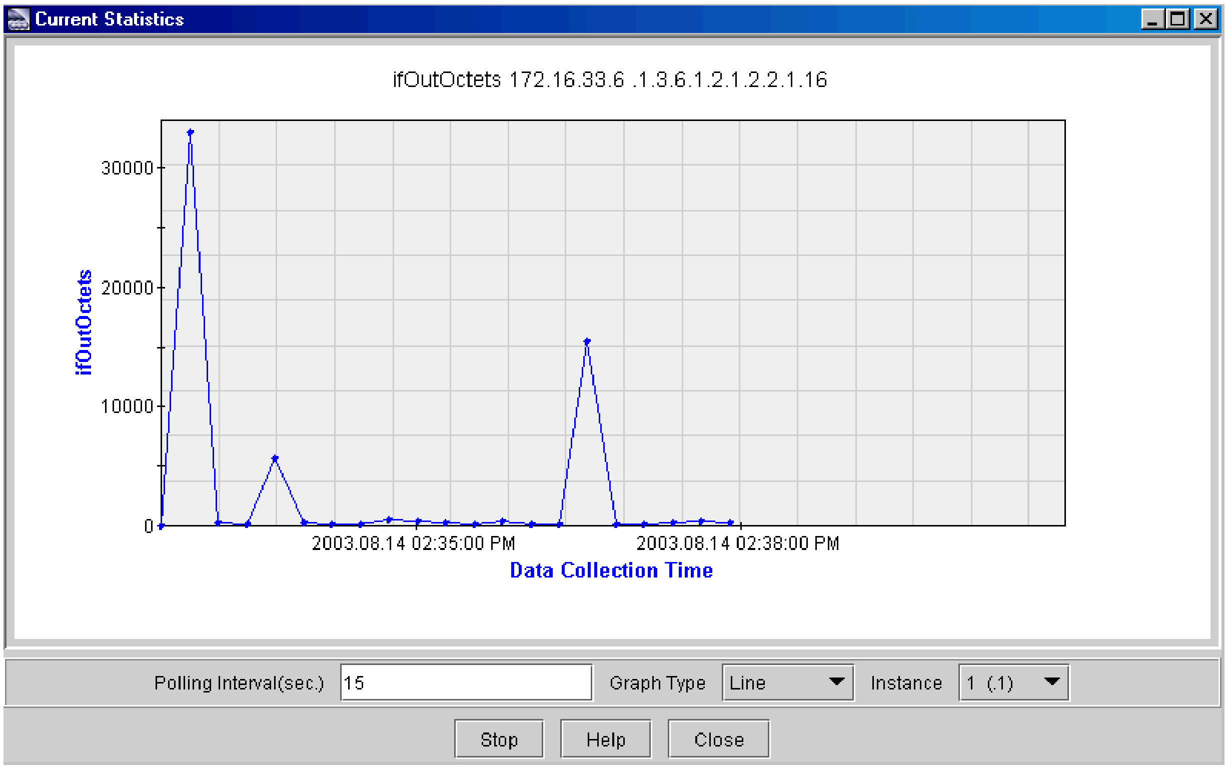
   By default, the data collection interval shown in the graph is 15 seconds. You can specify the required polling interval in seconds. Decrease the value if very close monitoring of a statistic is needed. This helps you in analyzing the effect of changes in intervals on data collection. But every time you change the interval, follow these steps:

   1. Click the **Stop** button.
   2. Change the interval.
   3. Click **Restart**. This helps you analyze the effect of change of time over data collection.
   4. Change Graph type.

2. You can choose to view the data as a bar or line graph as you monitor the collected data. When small values are plotted, line graphs can be difficult to view. In such cases, you can immediately change to a bar graph.

Follow these steps to view Current Statistic Graph:

1. In the Configured Collection panel, select the Statistic for which you want to monitor in real time.
2. Select *View -> Plot -> Current Statistic* from the Panel-Specific Menu Bar. You will see the following figure.



Polling Interval(sec.) 15
Graph Type Line
Instance 1 (.1)

FIGURE 25-4 Plotting Current Statistic

You can change the Polling Interval and Graph Type and see the results change.

25.4 Threshold Notification

25.4.1 Overview

Performance monitoring involves the following concepts:

- Data is collected from agents of network devices and stored.
- The collected data is cross-checked with threshold values. If it exceeds the limits of the threshold values, a notification can be sent to the user indicating that network performance is degrading.

A threshold has the following:

- a value
- a type (Max, Min or Equal).

  For example, if type is set to Max, the Threshold is exceeded when the collected value goes above the threshold value.
- a message that is to be generated when the threshold is exceeded.
- a value at which the threshold is reset

Thresholds are defined and associated with Statistics. A single Statistic can have many thresholds indicating a severity, such as Critical, Major, Minor, etc. Whenever data are collected for the statistic, it is cross-checked with the associated thresholds. If the collected value exceeds the thresholds, the threshold message is displayed as an Event in Fault Management.

Note: If multiple thresholds are associated with a Statistic, then the collected value will be checked with every threshold value. For every threshold value exceeded, its corresponding message will be displayed.

25.4.2 Example

Assume a Statistic called Interface_in_octet for the switch named switch_vg3w. For efficient performance of the switch, the value of this statistic must be between 1300 and 1370. This means that you should have some notification mechanism to inform you when the statistic value is not within this limit.

Define three thresholds for this statistic:

switch_vg3w-critical, switch_vg3w-major, and switch_vg3w-minor, as shown in the following table.

TABLE 25-3 **Threshold Example**

Threshold Property	Switch_vg3w-minor	Switch_vg3w-major	Switch_vg3w-critical
value	1320	1350	1371
type	max	max	max
threshold message	Has entered violation stage	Monitor the value; it might exceed critical threshold	Reached critical point. Immediate attention required.
reset value	1319	1349	1369

In short, if the Statistic value is 1350, the threshold switch_vg3w-major is exceeded. The message “Monitor the value; it might exceed critical threshold” will be generated. But if the statistic value goes below 1369, the threshold will be reset and, again, data collected for the Statistic will be monitored.

25.4.3 Threshold Interactions

- The reset value plays an important role. Once a threshold is exceeded, until the collected value reaches the threshold's reset value, the threshold will be in that severity state itself. As soon as the value reaches the reset value, the threshold is reset until the threshold is exceeded again.

- If another threshold exists of a lower severity and if the collected data falls in its limits, that threshold will generate the message.
- If another threshold exists with higher severity, the higher severity threshold will take precedence and its message will be displayed. The threshold with lower severity loses its importance and will not be generated until the threshold with the higher severity reaches its reset value.

25.4.4 Viewing Thresholds on the Network Events Screen

Once the collected value for a Statistic exceeds threshold limits, a notification is sent to the Fault module of the AlliedView NMS. The fault module receives this notification and displays it on its Network Events panel.

Note: You can see the number of events that have been generated of different severity in the Alarm count by severity panel. Clicking on a number will display the associated alarms. The colors denote the severity (Red means Critical, Orange means Major, etc.).

25.5 Configuring Statistics

When setting up the AlliedView NMS, an Administrator will have to set up polling objects and polling filters so that the polled data (Statistics) are written to the AlliedView NMS database as polled data (Statistics) and can be extracted to provide real-time or historical reports. Once a AlliedView NMS system has been in service for a period of time, additional statistics may be needed. This can be done by modifying the appropriate polling object or creating a Statistic for specific node.

To add a statistic, select *Edit ->Add Statistic* from the Panel-Specific Menu Bar. The Modify Polled Data form appears.

26. Setting Up Performance Management

Performance monitoring basically means collecting useful data from network devices and determining how efficiently the network is functioning. *Performance* is measured based on factors such as:

- Number of bytes of data received (over a period) by a particular interface of a device.
- Number of bytes of data sent (over a period) by a particular interface of a device.
- An estimate of the interface's current bandwidth in bits per second.

The data pertaining to a network device are collected based on the definition of performance variables (called **Statistics**).

Note: During startup, the AlliedView NMS server creates a set of default statistics that are inactive. Figure 26-1 shows these default Statistics.

Once the AlliedView NMS server starts, data collection starts automatically. Data is collected from the devices listed under the **Hosts** list in the Configured Collection panel, as shown in Figure 26-1. Data is collected only for those Statistics listed in the panel that have been defined.

Performance configuration involves a series of steps that must be understood in sequence so that the Administrator can ensure that all devices in the network are operating efficiently and that any degradation in performance is reported to users as quickly as possible. Once the purpose of these steps is explained, the specific tasks can be shown.

Overall, performance management involves three main areas:

1. Data Collection

   To configure data collection means to define from which devices (managed objects) data will be collected, what data to collect, and how the data will be filtered before it is stored in the database.

2. Threshold Configuration

   As the data is collected and scored, it needs to be checked against threshold values to provide a method to see that the device performance is degrading.

3. Reporting

   As the data is collected and thresholds are checked, users must be notified.

The settings for Performance Management are in a set of configuration files (**.conf**) in Extended Markup Language (XML) format.

Warning: Editing configuration files directly should only be done under the supervision of Allied Telesis support personnel, since it is very easy to delete or change data collection that would result in a loss of performance monitoring for devices. Use the forms and menus described in this section to set up Performance Management.

Use the following table to locate the task you wish to perform. Use the screen or form name to locate the relevant section.

TABLE 26-1 Task List for Performance Monitoring

Task	Screen / Form Name (if Applicable)	Section
Data Collection Screen	Configured Collection	("Screen Components for Statistics" on page 975)
Data Collection (Statistics) - Overview - Create Polling Filters - Create Statistic	Create, Modify, Delete DataCollection Detailed Properties	("Data Collection" on page 977) ("Polling Objects" on page 978) ("Add a Statistic" on page 982)
Thresholds - Overview - Configure Thresholds - Associate Threshold with Statistic	Threshold Properties Threshold Properties	("Threshold Notification" on page 985) ("Add Threshold" on page 987) ("Associate Thresholds with Statistics" on page 989)

26.1 Data Collection Screen

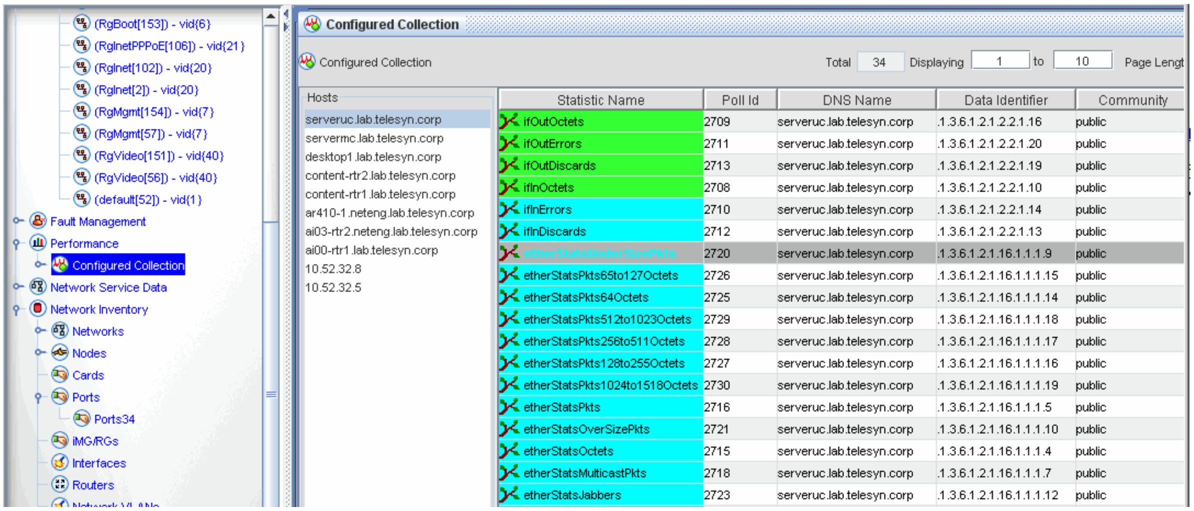
You can view the list of statistics associated with each of the ManagedObjects discovered in the network via the **Configured Collection** panel.

Note: *A Managed Object (MO) represents a network element for which data has to be collected. It can be a node, interface, a port, a card, a slot, etc.*

26.1.1 Screen Components for Statistics

To access the Data Collection screen, perform the following:

1. Select Configured Collection node from the tree in the left frame. You can see the Configured Collection panel in the right frame, which displays a list of nodes under the **Hosts** column. This list indicates that these ManagedObjects have been identified in the network for data collection.
2. Select any of the hosts, and you will see the associated Statistic. (Each row of information is called a Statistic). Refer to the following figure.



Configured Collection

Total 34 Displaying 1 to 10 Page Lengt

Hosts
serveruc.lab.telesyn.corp
servermc.lab.telesyn.corp
desktop1.lab.telesyn.corp
content-rtr2.lab.telesyn.corp
content-rtr1.lab.telesyn.corp
ar410-1.neteng.lab.telesyn.corp
ai03-rtr2.neteng.lab.telesyn.corp
ai00-rtr1.lab.telesyn.corp
10.52.32.8
10.52.32.5

Statistic Name	Poll Id	DNS Name	Data Identifier	Community
ifOutOctets	2709	serveruc.lab.telesyn.corp	.1.3.6.1.2.1.2.2.1.16	public
ifOutErrors	2711	serveruc.lab.telesyn.corp	.1.3.6.1.2.1.2.2.1.20	public
ifOutDiscards	2713	serveruc.lab.telesyn.corp	.1.3.6.1.2.1.2.2.1.19	public
ifInOctets	2708	serveruc.lab.telesyn.corp	.1.3.6.1.2.1.2.2.1.10	public
ifInErrors	2710	serveruc.lab.telesyn.corp	.1.3.6.1.2.1.2.2.1.14	public
ifInDiscards	2712	serveruc.lab.telesyn.corp	.1.3.6.1.2.1.2.2.1.13	public
etherStatsUnderSizePkts	2720	serveruc.lab.telesyn.corp	.1.3.6.1.2.1.16.1.1.1.9	public
etherStatsPkts65to127Octets	2726	serveruc.lab.telesyn.corp	.1.3.6.1.2.1.16.1.1.1.15	public
etherStatsPkts64Octets	2725	serveruc.lab.telesyn.corp	.1.3.6.1.2.1.16.1.1.1.14	public
etherStatsPkts512to1023Octets	2729	serveruc.lab.telesyn.corp	.1.3.6.1.2.1.16.1.1.1.18	public
etherStatsPkts256to511Octets	2728	serveruc.lab.telesyn.corp	.1.3.6.1.2.1.16.1.1.1.17	public
etherStatsPkts128to255Octets	2727	serveruc.lab.telesyn.corp	.1.3.6.1.2.1.16.1.1.1.16	public
etherStatsPkts1024to1518Octets	2730	serveruc.lab.telesyn.corp	.1.3.6.1.2.1.16.1.1.1.19	public
etherStatsPkts	2716	serveruc.lab.telesyn.corp	.1.3.6.1.2.1.16.1.1.1.5	public
etherStatsOverSizePkts	2721	serveruc.lab.telesyn.corp	.1.3.6.1.2.1.16.1.1.1.10	public
etherStatsOctets	2715	serveruc.lab.telesyn.corp	.1.3.6.1.2.1.16.1.1.1.4	public
etherStatsMulticastPkts	2718	serveruc.lab.telesyn.corp	.1.3.6.1.2.1.16.1.1.1.7	public
etherStatsJabbers	2723	serveruc.lab.telesyn.corp	.1.3.6.1.2.1.16.1.1.1.12	public

FIGURE 26-1 Collection View Panel

The following table lists the components in.the following figure.

TABLE 26-2 Data Collection Screen Components

Component	Description for Data Collection Screen Components
Property Columns	For every statistic the associated properties are displayed in columns, such as Statistic name, Poll ID, Data Identifier, DNS Name, interval etc. Some of the properties are as follows: **Statistic Name** - A string to identify the Statistic uniquely. This should be a meaningful name describing the Statistic. **Poll ID**: A unique number associated with each Statistic to identify the Statistic. Poll ID is automatically generated so no two Statistics will have the same Poll ID. **DNS Name**: This is the Host name (device name) with which this Statistic is associated. **Data Identifier**: This is the Identification number of the device interface from which data about the device is to be collected. This Data Identifier is otherwise called as OID and it is unique for every device. A list of possible OIDs for a device exists in the MIB definition of the device. *Note: To view the OIDs of nodes and interfaces for a device, use the MIB browser. Refer to Section "Built-in Browsers - SNMP MIB and CWMP" on page 1036* **Interval** - This specifies the time interval at which data should be collected for the Statistic. For example, the value 300 indicates that after every 300 seconds, data is collected.
Page Length	The drop-down box labeled Page Length displays a number of hosts to be displayed per page. By default, it is set to 10. Hence you can see ten hosts displayed in the left panel of the Configured Collection frame. You can select other values such as 20, 30, 40, 50 etc. and view that number of hosts together.
From and To Range	There are two text boxes available labeled Displaying and To. You can set values in these, press Enter, and see the hosts list in that range. For example, if you set **Displaying** as 4 and **To** as 13, then you will be able to view from Host 4 to Host 13. By default, the hosts are displayed in reverse alphabetical order.

TABLE 26-2 Data Collection Screen Components (Continued)

Component	Description for Data Collection Screen Components
Navigation Buttons	You can see four navigation buttons provided at the top right of the frame. They are Go to first page, Go to previous page, Go to next page and Go to Last page respectively. They will get automatically enabled and disabled based on your choice of page length and total number of hosts.
Total	This text box cannot be edited and it shows the total number of hosts available for data collection.

Note: The green branch-like image adjacent to the Statistic name denotes the type of Statistic. Statistics are of three types: Node, Interface, and Multiple. The symbol with multiple branches denotes that the statistic is of type Multiple. (A multiple type contains one node and all interfaces.)

If no data are to be collected for a Statistic, the data are disabled temporarily. In such a case, the Statistic row is displayed in blue color. Once it is activated, the row color changes to green.

Note: You can see the number of events that have been generated of different severity in Alarm count by severity panel.

26.2 Data Collection

Data collection is done using the flowchart shown in the following figure.

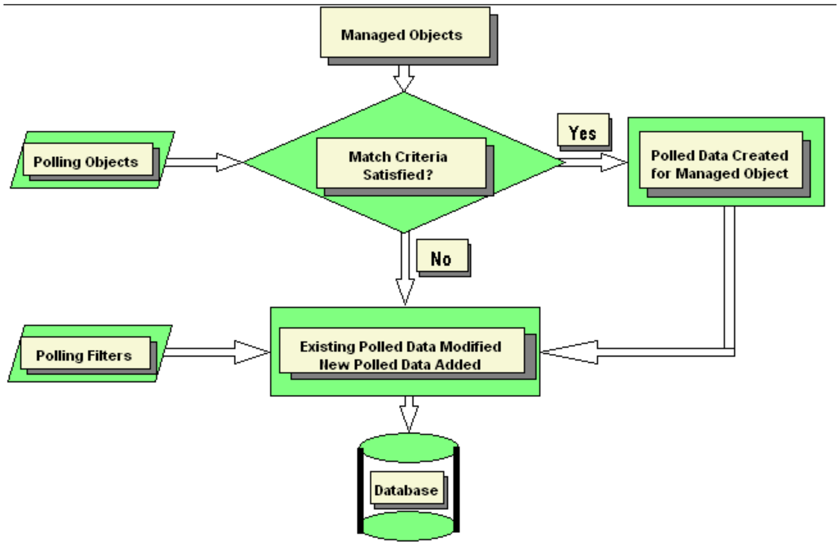

Managed Objects
Polling Objects
Match Criteria Satisfied?
Yes
Polled Data Created for Managed Object
No
Polling Filters
Existing Polled Data Modified New Polled Data Added
Database

FIGURE 26-2 Data Collection Flow

The flowchart elements are as follows:

- Managed Object - Created by the Topology feature, it is an entity that represents a device or part of a device (such as a port, card, or interface), and has properties.
- Polling Object - Created by Performance Management, it is an object that has two properties:
  - Match Criteria
  - Data Collection Criteria
- Polled Data - The actual name (statistic) for the data to be collected in the database. Examples would be **Interface_In_Octets** or **Ether_History_Octets**.

- Poll Filter - The Polled Data for the Managed Object is filtered so that existing polled data can be modified/deleted, or new polled data can be added.

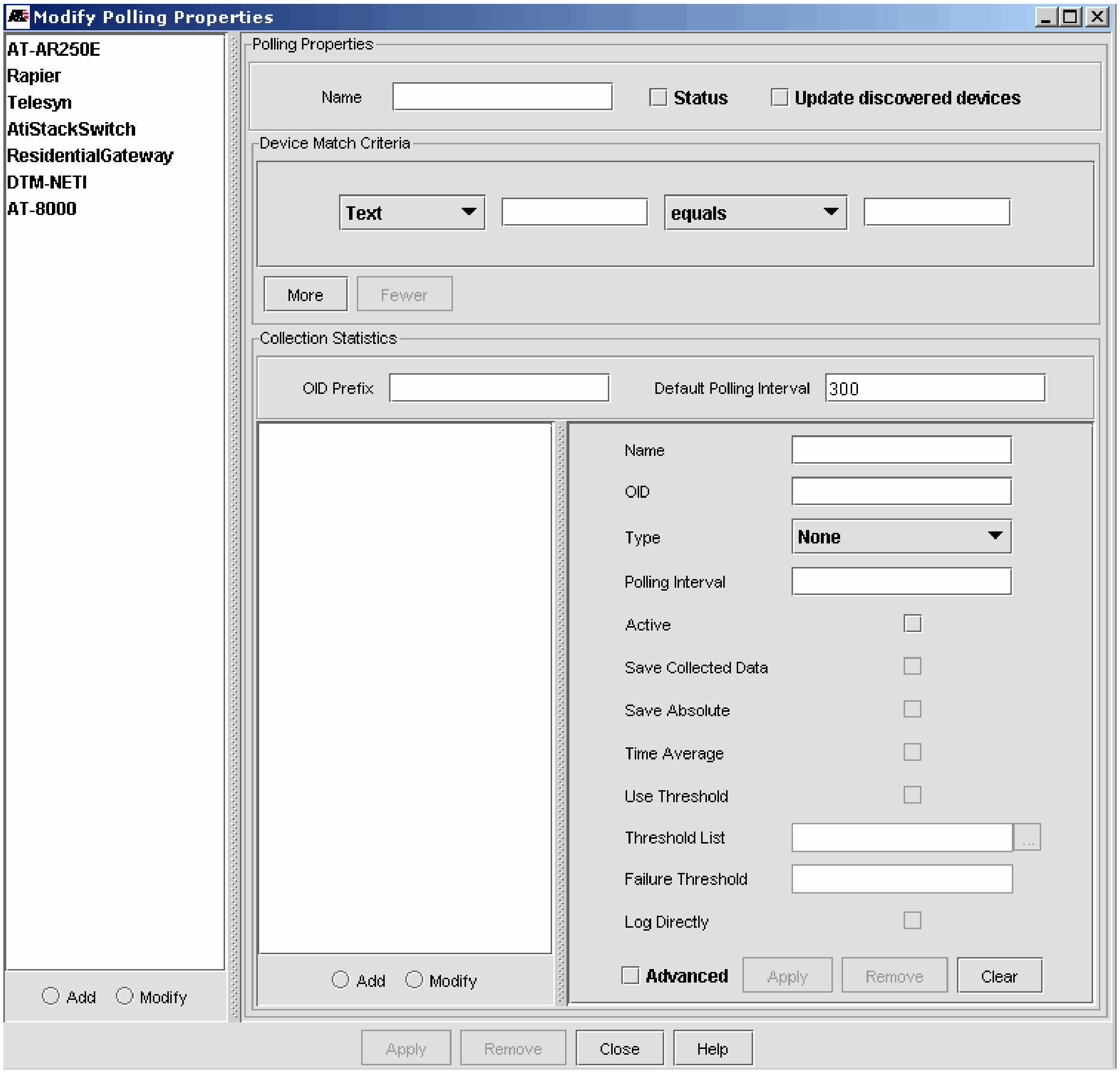
When the server starts up, the definitions in the AlliedView NMS internal files are used as follows:

1. Polling Objects are created based on a AlliedView NMS internal file. Each Polling Object has the two criteria, Match and Data Collection.
2. When Topology creates a Managed Object, the MO is passed through the Polling Object, where the properties of the MO are compared to the match criteria of the Polling Object.
3. If there are match criteria, PolledData is created for entry in the Data Collection criteria.
4. If there are no Polling Filters, the PolledData goes directly to the database.
5. If there are Polling Filters, the PolledData is passed through the Polling Filter one by one and is modified as specified by the filter. Then the data can be sent to the database.

The following subsections show how to add these Performance Management modules.

26.2.1 Polling Objects

A Polling Object is used for creating a single collection point for multiple devices. To add, modify, or delete a Polling Object, select *Edit -> Polling Objects*. The following figure appears.



Text equals

Default Polling Interval 300

Type None

FIGURE 26-3 Modify Polling Properties Form - File

26.2.1.1 Adding a Polling Object

To add a polling object:

1. Select the **Add** radio button under the list of polling objects (left panel).
2. Fill in the fields under **Polling Properties** as follows:
   - **Name** - Required, a string to identify the Polling Object.
   - **Status** - Checked means active and so the data collection for the associated Polled Data can be done. When unchecked, data collection for associated Polled Data is stopped. Default is checked.
   - **Update Discovered Devices** - Checked means the Polling Objects definitions will be applied over existing MOs and they will updated with the information input here. If unchecked, the Polling Object will be used for newly created MOs only.
3. Specify at least one criteria under **Device Match Criteria** and set it against a string or numeric value. Following are the default set of MO properties:

- Global: status, type, managed,
- Boolean: isGroup, isContainer, isSNMP, is DHCP, isRouter, isNode, isNetwork, isInterface,
- System: sysName, sysOID,
- Interface: ifSpeed, ifDescr, ifIndex

Use the **More** and **Fewer** buttons to get the correct number.

Note: The Fewer button will remove the last criteria you added.

The criteria are set as an AND condition. To change this, define a **User Class.** Contact ATI support for examples of user class files on the AlliedView NMS Server.

4. Under **Collection Statistics**, select the **Add** radio button, and fill in the fields as described in the following table.

Note: Choosing the type and location of data from the MO is done through the MO's agent, which is the program that receives and processes the data request, and the Object Identifier (OID), which is the unique number that identifies that characteristic for the MO.The list of OIDs is retrieved from the MIB definition of the device. To view the OIDs for a device, use the MIB Browser tool.

TABLE 26-3 **Data Configuration Fields**

Field	Description
OID Prefix	Normally the Data identifiers are lengthy. For the identifiers that have in common the starting **n** digits, you can specify that as prefix. For example, assume two Statistics, IfSpeed and IfinOctect. The corresponding Data identifiers are .1.3.6.1.2.1.2.2.1.5.1 and .1.3.6.1.2.1.2.2.1.10.1. You can see the first part .1.3.6.1.2.1.2.2.1 is common to both, so you can specify the common prefix as **.1.3.6.1.2.1.2.2.1.** Even if you do not specify the prefix, Performance module will add the prefix to the identifier.
Default Polling Interval	The time interval for periodic data collection. For example, if set to 5, then for all the Data identifiers, data will be collected once in every 5 seconds. **Default** value: 300 seconds.
Name	Any meaningful string for the Data identifier. **Required**
OID	A unique Object Identifier string that represents a MIB entry. Data is collected for this identifier. An SNMP-specific Data identifier is called an **OID**. For example . 2.2.1.16.1 refers to IfInOctects interface instance 1. **Required**.
Type	This can be set to interface, node, multiple, or none. **Node** - Used when Data identifier is of type Scalar. If you choose the type to be **Node** you must specify the full OID. For example to collect data for Interface_in_octets instance 1 then choose this type and specify the data identifier as 2.2.1.10.1. **Interface** - Exclusively for IF table entries of RFC 1213 MIB, **only**. This is used when the data identifier has many instances.When you want to collect data for all the instances of an OID choose the type to be Interface. Enter the data identifier as 2.2.1.10. For every instance of the OID, a PolledData will be created. **Multiple** - This type can be used to collect data for OIDs that have multiple instances. As Interface type is specific to IF table entries for other OIDs that have multiple instance you can choose the type as Multiple. Only one PolledData will be created for the OID specified but data collection will be done for all the instances. **None** - Used when other protocols are used for data collection apart from SNMP. **Default** value: None.
Polling Interval	The time interval for periodic data collection. For e.g. if set to 2, it indicate that for all the Data identifiers, data will be collected once in every 2 seconds. **Default**: 300 seconds.

TABLE 26-3 Data Configuration Fields

Field	Description
Active	If you uncheck the checkbox, data collection will be temporarily stopped for this Data identifier. To resume data collection you will have to check this checkbox. **Default**: True (checked).
Save Collected Data	If unchecked, specifies data will not be stored, and can be viewed only by the Real Time monitoring using Current StatisticGraph you do not want to store the collected data, "uncheck" this check box. **Default**: True (Checked).
Save Absolute	This option is applicable only for Counter type OIDs. By default, data collected for Counter type OIDs is not stored as it is. The difference between the previous data and latest data is collected and stored. If the exact value (absolute value) of collected data has to be stored for Counter type OIDs then this check box should be checked.Data collected for OIDs of other data types are saved as absolute values. **Default**: False.
Time Average	If you check this checkbox then the Time Average will be calculated as (Latest collected value + Previous value) / Difference in Data collection Time value.This is mostly calculated for Counter type and Gauge type Data identifiers where the data collected will be an incremental value and at one point will reach the final value and reset to Zero. As this reset may happen soon and very often, it is preferred that a Delta value is derived from two consecutive Polls. **Default**: false.
Use Threshold	Check to apply threshold for this Identifier. **Default**: False (unchecked).
Threshold List	A list of thresholds to apply to this data. Click the ellipses (...) to get a pop-up list of applicable thresholds. Select the desired thresholds from the pop-up list (Shift+click to select multiple thresholds), and then click **OK** in the pop-up window.
Failure Threshold	Number of consecutive failures after which the threshold event should be generated. This can be used where a single Poll (Datacollection for the Data identifier) is not stable. For example, assume the Data identifier has a threshold associated and it is predicted that the data collected can be crosschecked 3 times. If the collected value still exceeds the Threshold value then it means that the collected data is stable and this may result in Performance degradation. **Default**: 1.
Log Directly	This option allows the polled data to be saved directly to a text file (comma-separated). The text file will be located in the NMS Server installation directory on the NMS host machine and will be named <device name or IP address>_<polled data name>.txt (e.g. **172.16.33.2_ifInOctets.txt**). *Note: This option is useful for quickly viewing the raw values as they are collected form polling but should not be used for long term data collection to avoid filling up the NMS server disk storage.*

After filling in these fields for an Identifier, click **Apply** and it will be added to the Data Identifier List. Once added, you can click **Modify** to modify the Identifier or **Remove** to remove it.

Once all the Identifiers have been configured, click **Apply**. This adds the Polling Object to the database and the statistic to the Configured Collection Panel.

26.2.1.2 Modify a Polling Object

Once set up, modifying the Polling Object will be necessary when you:

- Stop data collection for all the associated Polled Data
- Modify the properties of existing Data Identifiers
- Add new Data Identifiers to add to the Polled Data

To modify a Polling Object, select *Edit -> Polling Objects,* and then perform these steps:

1. Select the polling object from the left panel, and then select the **Modify** radio button just below the list.

2. Under Polling Properties, change the **Active** and **Update Managed Objects** checkboxes, if desired.

Note: The information under Device Match Criteria is not editable.

3. Under **Collection Statistics**, select a Data Object from the list and change the field values as needed.

Note: Check the Advanced checkbox to enable all of the fields and checkboxes, if necessary.

Repeat for each Data Object you need to change.

4. When you are done, click **Apply** to make the change to the database.

26.2.1.3 Delete a Polling Object

Deleting a Polling Object means to delete all the statistics associated with the Data Identifiers.

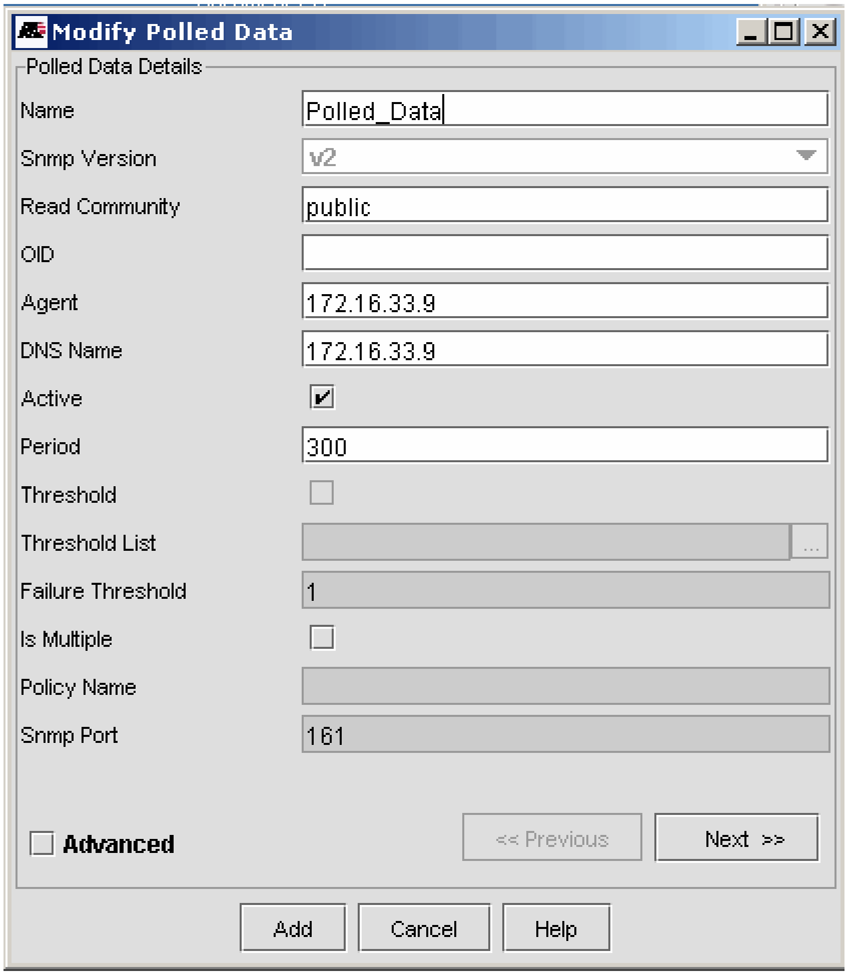
To delete the Polling Object, select *Edit -> Polling Objects,* and then perform these steps:

1. Select the Polling Object on the left panel, and then select the Modify radio button just below the list.
2. Click the **Remove** button at the bottom of the form. A confirmation box asks to confirm the delete.
3. Click **Yes** and the Polling Object will be removed from the left pane.

You can view the results in the Configuration Collection panel, where the Statistics associated with the Polling Object are deleted.

26.2.2 Add a Statistic

A Statistic may need to be added to a specific device. For such small changes, select *Edit -> Add Statistic*. The **Modify Polled Data** form will appear, as shown in Figure 26-4.



Modify Polled Data

Polled Data Details

Name	Polled_Data
Snmp Version	v2
Read Community	public
OID	
Agent	172.16.33.9
DNS Name	172.16.33.9
Active	☑
Period	300
Threshold	□
Threshold List	
Failure Threshold	1
Is Multiple	□
Policy Name	
Snmp Port	161

□ Advanced

FIGURE 26-4 Data Collection for Adding a Statistic

The following table lists the properties and descriptions.

TABLE 26-4 Properties for Adding a Statistic

Property	Description
Name	Any meaningful string for the Data Identifier. **Required**.
SnmpVersion	One of the three SNMP versions - VI, V2 or V3. **Required**.
Read Community	Enter the string with which the devices are identified in a network. Most of the equipment vendors set the Community value as **public** for their devices, so it is usually used here. Otherwise you have to check the string used for the particular device. *Note: The community specified must be enabled on the device.*
OID	A unique Object Identifier string that represents a MIB entry. Data is collected for this identifier. An SNMP specific Data identifier is called an **OID**. For example, 2.2.1.16.1 refers to IfInOctects interface instance 1. **Required**.
Agent	Normally a device will have one agent in it to collect device data, and the device name and agent name will be the same. **Required**.
DNS Name	Name of the device from which data have to be collected.

TABLE 26-4 Properties for Adding a Statistic (Continued)

Property	Description
Active	If you uncheck the check box, the data collection will be stopped for this OID. (The statistic row once created will be blue.) To activate data collection, check the box. Default value: True (checked).
Period	The time interval for periodic data collection. For example, if set to 2, for all the Data identifiers, data will be collected once in every 2 seconds. Default value: 300 seconds.
Threshold	Checking means the Threshold will be applied on this Data identifier. Unchecked means no Threshold will be applied. Default value: False (unchecked).
ThresholdList	Name of the Thresholds in comma separated format, thus associating them to this Data identifier for monitoring data collection.
Failure Threshold	Threshold at which a failure is declared.
isMultiple	Checking means the data identifier is of type multiple.
Policy Name	The name of the polling policy.
Snmp Port	Specify the Port No over which device data is passed to the AlliedView NMS by the device agent. The default SNMP agent port is 161. **Required**.
Advanced	Allows the optional values to be modified.
Protocol	SNMP, TL1 or any other protocol used by you for data collection.The default protocol **SNMP** will be assumed for data collection.
Save	Whether to view the data only by Real Time monitoring using Current Statistic Graph. To specify that you do not want to store the collected data, uncheck this check box. Default value: True (Checked).
saveAbsolutes	This option is applicable only for Counter type OIDs. By default, data collected for Counter type OIDs is not stored as it is. The difference between the previous data and latest data is collected and stored. If the exact value (absolute value) of collected data has to be stored for Counter type OIDs, then this check box should be checked. Data collected for OIDs of other data types are saved as absolute values. Default value: False (Unchecked).
SaveOn Threshold	Possible values are true and false. If true the collected data is saved only when it exceeds the threshold. Default value: false
Time Average	Checking means the Time Average will be calculated as follows: (<Latest collected value> + <Previous collected value>) / <Difference in data collection Time value> This is mostly calculated for counter type and gauge type OIDs where the data collected will be an incremental value and at one point will reach the final value and reset to zero. As this reset may happen soon and very often, it is preferred that a delta value is derived from two consecutive polls. Default value: false.
Last Counter Value	The counter value last read.
Last Time Value	The time the counter was last read.
Next Time Value	The next time the counter will be read.

TABLE 26-4 Properties for Adding a Statistic (Continued)

Property	Description
Log Directly	Checking means to store the collected data in flat files rather than storing them in database. Default value: false (unchecked).
Log File	The log file name with a full path (the location on the hard disk as where the log file has to be stored).
parentObj	Name of the Managed Object which acts as the parent for this Data Identifier.
Poll ID	A unique number associated with each Statistic to identify the Statistic. Poll ID is automatically generated so no two Statistics will have the same Poll ID.
Advanced	Allows the optional values to be modified.

26.2.2.1 Modify a Statistic

To modify a Statistic, in the Configured Collection table, select a Statistic, and then select *Edit -> Modify Statistic*. In the editable fields of the **Polled Data Details** form, make the appropriate changes (refer to "Add a Statistic" on page 982), and then click **Modify**. The changes are made immediately.

An example would be to check the **Active** checkbox. Clicking **Modify** would make the statistic active and the row would turn green.

26.2.2.2 Remove a Statistic

To delete a statistic in the Configured Collection table, select a Statistic, and then select *Edit -> Remove Statistic*. A confirmation dialog box will appear. Once the **Yes** option is clicked in the confirmation dialog, the Statistic is deleted from the database.

26.2.2.3 Example of Adding a Statistic

To add a Statistic, perform the following steps:

1. In the Configured Collection panel, select the device on which you want to add the statistic.
2. Select *Edit -> Add Statistic* from the menu. The form shown in Figure 26-4 will appear.
3. Enter a name for the statistic in the **Name** field.
4. Enter the OID for the value to be polled in the **OID** field.
5. Uncheck the **Active** checkbox if you do not want this statistic to be active at this point.
6. Check the **Advanced** checkbox, then set the threshold values as needed.
7. Click **Next**.
8. If not already checked, check the **Advanced** checkbox, and then change the values as needed.
9. Click **Add**. Your new statistic will appear in the Configured Collection panel. If **Active** was checked, it will be enabled (green).

26.3 Threshold Notification

Performance monitoring involves two concepts:

- Data is collected from agents of network devices and stored.
- The collected data is cross-checked with threshold values. If it exceeds the limits of threshold values, a notification can be sent to the user indicating that network performance is degrading.

A threshold has the following:

- Value

- Type
  - Max - When collected data exceeds a value, report an error
  - Min - When collected data drops below a value, report an error
  - Equal - When collected data equals a value, report an error
- What message should be generated when the threshold is exceeded.
- At what value should this threshold get reset.

Thresholds are defined and associated with statistics. A single statistic can have many thresholds indicating a severity such as Critical, Major, Minor, etc. Whenever data is collected for the statistic, it is cross-checked with the associated thresholds. If the collected value exceeds the thresholds, then the threshold message is displayed.

Refer to the following figure.

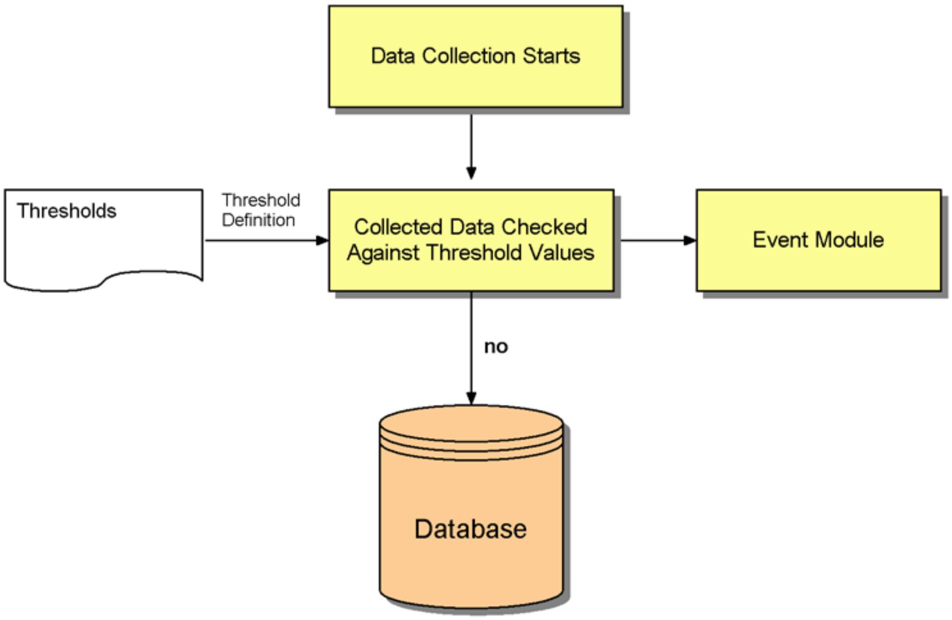


FIGURE 26-5 Threshold Processing

Thresholds can be created, modified, or deleted directly in the AlliedView NMS internal file by defining the attributes of the thresholds.

Warning: Editing configuration files directly should only be done under the supervision of Allied Telesis support personnel, since it is very easy to delete or change thresholds that would result in a loss of threshold monitoring for devices. Moreover, any changes in one file need to be coordinated with changes in other files. Use the forms and menus described in this section to set up thresholds.

There are three threshold types:

- Long Values

  Thresholds can be associated with Data identifiers for which data collected is of type long. Some of such sample Data identifiers are IfAdminStat, IfOperStat etc. in RFC 1213 MIB. The value you provide for this Threshold will be compared as it is with data collected for the identifier.

- String Values

  Thresholds can be associated with Data identifiers for which data collected is of type string. An example is SysDescr. To monitor a change in system description use String Thresholds.

- Percentage Values

  Assume you want to set the number of pages to be loaded in a printer to depend on the Toner level. Moreover, when the toner level is 80% of the number of pages to be printed, you wish to be notified. To achieve this, you create a Percentage Threshold with a value 80. Collect data for two Statistics, Toner level and Number of pages in the printer. Divide the first by the second to find the percentage. If the resulting value exceeds the Threshold value (80), then you will receive notification. The steps are:

  1. Data will be collected for first statistic.
  2. When compared with Threshold value, if Threshold type is percentage, for the associated statistic (second statistic) data will be collected.
  3. Both will be divided and result multiplied by 100, thus giving a percentage.

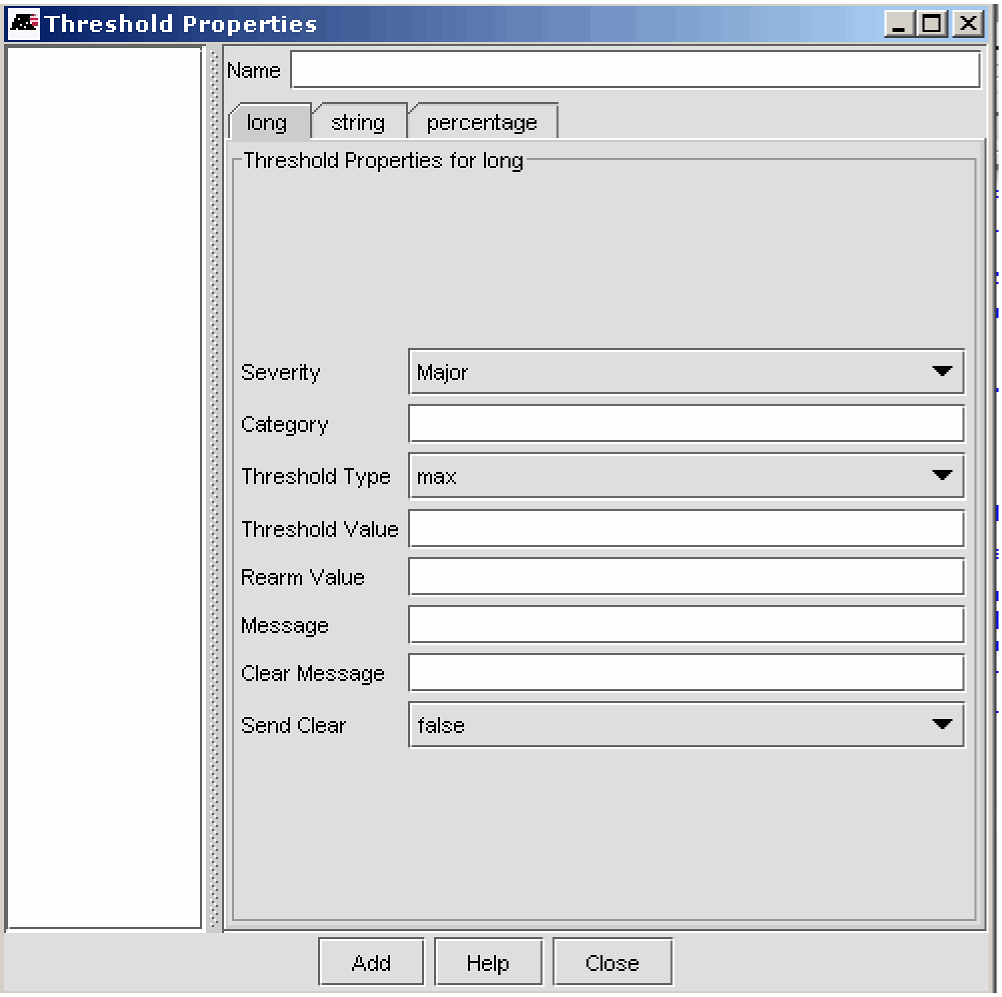
The notification that you receive when the collected value exceeds the Threshold value is in the form of a Threshold Event. An event is an occurrence of some action. Hence, whenever the Threshold value is exceeded, a Threshold event will be generated, which will be handled by AlliedView NMS Fault module. Also, every Threshold event is associated with a Severity to denote the criticality of the situation. For example, a severity of Critical should indicate that immediate attention is needed on data collection.

You can associate multiple thresholds with a single Statistic. Doing so allows you to control every value collected. For example, you can say if the collected value is above 10, the severity is minor. If the collected value is above 20, severity is major. In such a case the following will happen:

1. Until a threshold reaches it's reset value, it will be in that severity state itself. As soon as it reaches the reset value, the threshold gets reset and waits for the collected data to again exceed its limit.
2. If another threshold exists of lower severity and if the collected data falls in its limits then that threshold will generate the message.
3. If a threshold exist with higher severity, the higher severity threshold will take precedence and its message will be displayed. The threshold with lower severity loses its importance and will not be generated until the threshold with a higher severity reaches reset state.

26.3.1 Add Threshold

To add a Threshold, access the Configuration Collection view, and then select *Edit -> Threshold -> Add Threshold*. The following figure appears, showing three tabs, one for each type of threshold. Type **long** is the default tab. The tabs are for long, string, and percentage properties. Refer to the following figure.



Threshold Properties

Name

Threshold Properties for long

Severity: Major

Category:

Threshold Type: max

Threshold Value:

Rearm Value:

Message:

Clear Message:

Send Clear: false

FIGURE 26-6 Threshold Properties (type long)

The following table lists the properties for the threshold form.

TABLE 26-5 Properties for Thresholds

Property	Description
Name	Any action in a network can be captured and an appropriate name can be given to the event generated on such actions. For example, when ManagedObjects are added into the database an event can be generated. This event may be named as **AddMOevent**. Similarly generated Threshold events can be named which is decided by the Administrator. This name will be used by the Fault module for Event handling and for appropriate notification.
Severity (Trigger Severity)	String to emphasize the importance of the event generated when the Threshold value is exceeded. By default, the following severity strings have been defined Critical, Major, Minor, Warning, Clear.
Category	By default, the word **Threshold** is used for identifying Threshold events.

TABLE 26-5 Properties for Thresholds (Continued)

Property	Description
Threshold Type	Type of Threshold value you are going to specify. Possible values are Max, Min or Equal: **Max** - If Collected value exceeds Threshold value, an event will be generated. **Min** - If Collected value is less than Threshold value, an event will be generated. **Equal** - If Collected value is equal to Threshold value, an event will be generated.
Threshold Value	Integer value which can be interpreted in two ways: 1. In the case of a Threshold defined for Long values, the data collected for the OID is compared with this value. 2. In the case of Percentage Thresholds, the result of (first OID / secondOID) * 100, a percentage value, is compared with this value.
Rearm Value	Integer which denotes that when the collected value (or calculated value in case of percentage thresholds) reaches the Rearm value, the violated Threshold is brought back to normal and a clear event will be generated.
Reset Severity	When the Threshold is reset, by what severity it should be denoted.
Allowed Values	String value which will be compared with the string data collected. If both match then a Threshold event will be generated. The string which you can specify here can be: - simply a string, for example router5. - a comma separated list, for example router1, router2. - using wild card characters, for example router* where * indicates any number of characters and any character.
Disallowed Values	String which will be compared with the string data collected. If both match then a Threshold event will be generated denoting a **reset** of Threshold. You can enter strings as specified above.
ObjectID	The Object Identifier for which data will be collected in case of PercentageThresholds.For example, 2.2.1.16.1.
Object ID Type	Type of Data identifier whether it is Node, Interface or Multiple.
Message	String that will be displayed in the Event panel of Fault module when Threshold value is exceeded.
Clear Message	String that will be displayed in the Event panel of Fault module when Threshold is reset (cleared).
Send Clear	Only when this check box is checked, Clear events will be generated on Threshold reset. Otherwise the Threshold will be reset and you will not know, as no information will be displayed in Event panel of Fault module.

26.3.2 Associate Thresholds with Statistics

When Statistics are created, thresholds can be associated with them. In the Configuration Collection panel, select *Edit -> Modify Statistic*. The form shown in Figure 26-4 appears.

1. In the first screen, check the **Advanced** checkbox.
2. Check the **Threshold** checkbox.
3. In the Threshold list text box, enter the threshold names separated by a comma.
4. Click **Modify** to make the changes. The threshold is activated immediately.

Note: *If you wish stop the monitoring of the statistic (usually for a short time), uncheck the Threshold box and select Modify.*

Note: *You cannot modify the threshold values from this dialog box.*

27. Setting Up Fault Management

Network Events are entities that represent the various happenings in the network devices. Events can convey general information or the current status of the devices in a network.

There are many powerful tools that allow an Administrator to control how managed objects (specific aspects of a device) report changes in their state. Through parsing and filtering, the Administrator can ensure that any change of state in a device or set of devices is reported in such a way that users can easily pinpoint the problem (or potential problem).

27.1 Fault Management Configuration

Note: Although the overall management area is called Fault Management, changes that explicitly result in an alarm on the Fault Management GUI (table) make up only a part of the overall Fault Management area. This is explained and shown below.

As a device or the AlliedView NMS undergoes a change, there are various mechanisms that inform the AlliedView NMS that a change has occurred. These reports pass through various software tools that process these reports and display the changes in a way that allows the user to quickly understand the nature, severity, and location of the change. Moreover, the user can edit these software tools to control the filtering and reporting format of these reports.

Figure 27-1 shows the overall configuration of Fault Management, the categories of device (and the NMS) changes, the software tools used by the NMS, and the areas where the results are displayed.

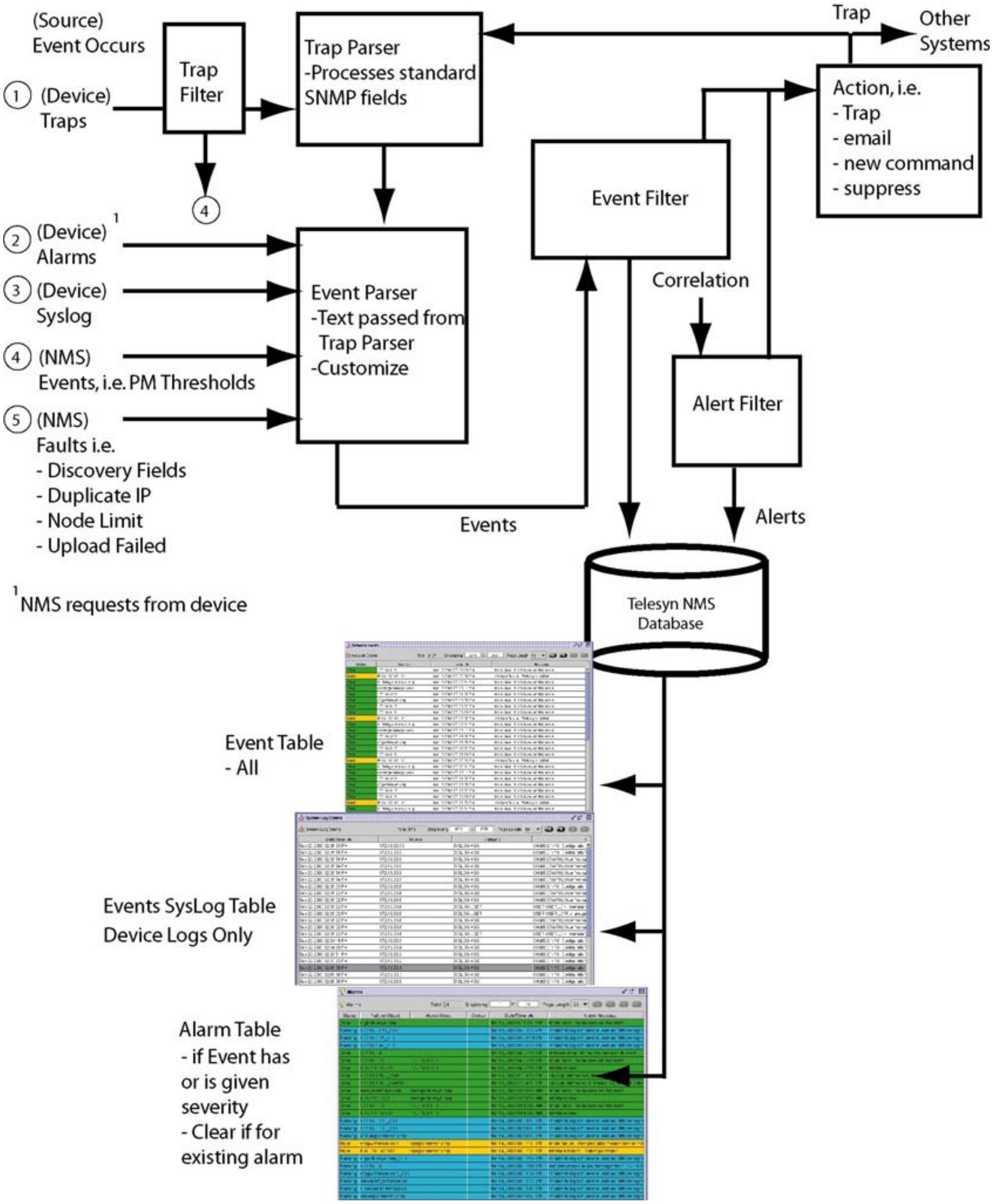


FIGURE 27-1 Fault Management Configuration for the AlliedView NMS

27.1.1 Task Overview

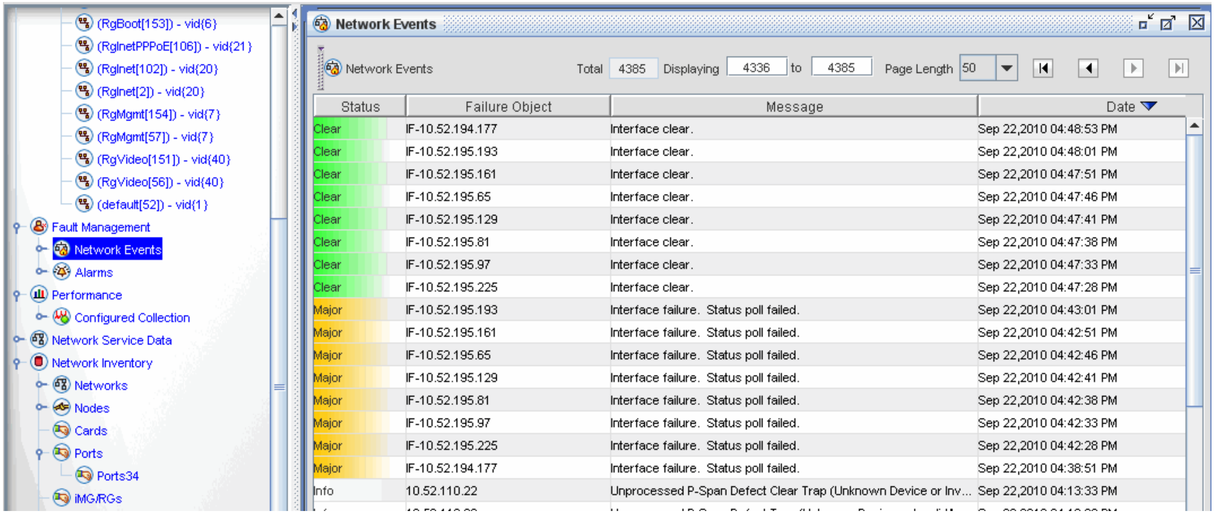
The following table lists the tasks that can be done at the Application interface. If you are using NMS, use the Screen Name as well to locate the relevant section.

TABLE 27-1 Task List for Fault Management

Task	Form/Screen Name (if Applicable)	Section
Review Events Screen	Network Events	(Event View)
Configure Trap Parsers	Telesis Trap Parser Configuration	(Configuring Trap Parsers)
Configure Event Parsers	Telesis Event Parser Configuration	(Configuring Event Parsers)
Configure Event Filters	Telesis Event Filter Configuration	(Configuring Event Filters)
Review Alarm Screen	Alarms	(Alarm View Display)
Alarm Propagation	Alarms	(Alarm Propagation)
Configure Alarm Filters	Telesis Alarm Filter Configuration	(Configuring Alarm Filters)
Configure System Logs	(System Log Configuration)	(Configuring System Logs)
Alarm Retrieval During (Re)Discovery	Retrieve Alarms	(Alarm Retrieval for iMAP Devices During Rediscovery)

27.2 Event View

This Event Viewer gets displayed on selecting the **Network Events** node under **Fault Management** in the AlliedView NMS Client Tree as shown in the following figure.



Network Events Total 4385 Displaying 4336 to 4385 Page Length 50

Status	Failure Object	Message	Date
Clear	IF-10.52.194.177	Interface clear.	Sep 22,2010 04:48:53 PM
Clear	IF-10.52.195.193	Interface clear.	Sep 22,2010 04:48:01 PM
Clear	IF-10.52.195.161	Interface clear.	Sep 22,2010 04:47:51 PM
Clear	IF-10.52.195.65	Interface clear.	Sep 22,2010 04:47:46 PM
Clear	IF-10.52.195.129	Interface clear.	Sep 22,2010 04:47:41 PM
Clear	IF-10.52.195.81	Interface clear.	Sep 22,2010 04:47:38 PM
Clear	IF-10.52.195.97	Interface clear.	Sep 22,2010 04:47:33 PM
Clear	IF-10.52.195.225	Interface clear.	Sep 22,2010 04:47:28 PM
Major	IF-10.52.195.193	Interface failure. Status poll failed.	Sep 22,2010 04:43:01 PM
Major	IF-10.52.195.161	Interface failure. Status poll failed.	Sep 22,2010 04:42:51 PM
Major	IF-10.52.195.65	Interface failure. Status poll failed.	Sep 22,2010 04:42:46 PM
Major	IF-10.52.195.129	Interface failure. Status poll failed.	Sep 22,2010 04:42:41 PM
Major	IF-10.52.195.81	Interface failure. Status poll failed.	Sep 22,2010 04:42:38 PM
Major	IF-10.52.195.97	Interface failure. Status poll failed.	Sep 22,2010 04:42:33 PM
Major	IF-10.52.195.225	Interface failure. Status poll failed.	Sep 22,2010 04:42:28 PM
Major	IF-10.52.194.177	Interface failure. Status poll failed.	Sep 22,2010 04:38:51 PM
Info	10.52.110.22	Unprocessed P-Span Defect Clear Trap (Unknown Device or Inv...	Sep 22,2010 04:13:33 PM

FIGURE 27-2 Network Events Main Panel

27.3 Configuring Trap Parsers

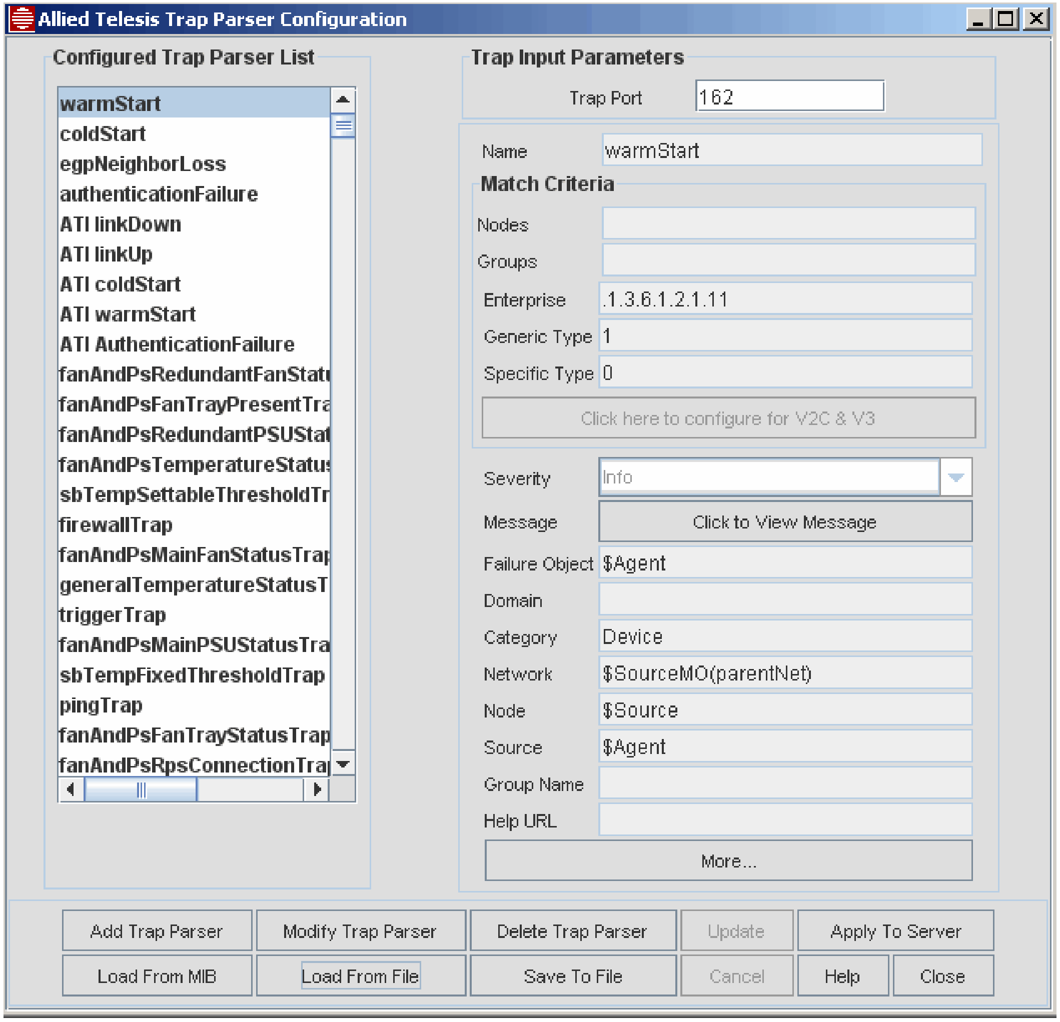
Configuring a Trap Parser is done to create and refine the information received from a trap (a specific unsolicited report by a device).

Configuring Trap Parsers can be done by using the information in the MIB to set the match criteria or defining the configuration and saving it to a file. (This requires that the MIB has been configured to include the traps. Refer to "Built-in Browsers - SNMP MIB and CWMP" on page 1036.)

Note: *Trap parsers are critical to alarm correlation and should only be changed under the supervision of Allied Telesis Technical Support personnel.*

To configure the Trap parser, select *Edit -> Configure -> Trap Parsers* from the main menu of the Network Events Panel.

The Trap Parser Configuration form is shown in the following figure.



Allied Telesis Trap Parser Configuration

Configured Trap Parser List

- warmStart
- coldStart
- egpNeighborLoss
- authenticationFailure
- ATI linkDown
- ATI linkUp
- ATI coldStart
- ATI warmStart
- ATI AuthenticationFailure
- fanAndPsRedundantFanStat
- fanAndPsFanTrayPresentTra
- fanAndPsRedundantPSUStat
- fanAndPsTemperatureStatu
- sbTempSettableThresholdTr
- firewallTrap
- fanAndPsMainFanStatusTrap
- generalTemperatureStatusT
- triggerTrap
- fanAndPsMainPSUStatusTra
- sbTempFixedThresholdTrap
- pingTrap
- fanAndPsFanTrayStatusTrap
- fanAndPsRpsConnectionTra

Trap Input Parameters

Trap Port: 162

Name: warmStart

Match Criteria

Nodes:

Groups:

Enterprise: .1.3.6.1.2.1.11

Generic Type: 1

Specific Type: 0

Severity: Info

Failure Object: $Agent

Domain:

Category: Device

Network: $SourceMO(parentNet)

Node: $Source

Source: $Agent

Group Name:

Help URL:

FIGURE 27-3 Trap Parser Configuration Form

Select a Trap Parser from the list to see how the fields are configured for that Trap parser. The following table describes these fields at a general level, as well as the option buttons. Many of the fields will have a variable name, discussed after this table.

TABLE 27-2 Trap Parser Configuration Form

Option	Description
Trap Port	Port that receives the trap. You must provide at least one, or the traps will not be received. More than one port can be entered, separated by commas.
Name	Name of the trap. The name should match the event.
Nodes	Specific nodes for this trap parser. Since most trap parsers are for general conditions or device types, this field is usually not used.

TABLE 27-2 Trap Parser Configuration Form

Option	Description
Groups	Grouping of nodes.
TrapOID	A TrapOID uniquely identifies an SNMP v2c or SNMPv3 trap and comes along with the Trap PDU. The TrapOID can be a match criteria. When the TrapOID has a value that starts with the Object Identifier the match criteria is met. Wildcard (*) can be used. When the Trap Object Identifier of the incoming trap must match exactly the TrapOID, put the value in brackets (<>).
Enterprise	Used to specify the enterprise OID of the SNMP v1 trap. If this field is specified, then the parser will be applied only if the trap enterprise field starts with the value you have specified. For example, when an enterprise OID is specified as **.1.3.6.1.2.1.11**, then **all** the OID's under this tree will be matched for traps. To avoid this kind of matching, the enterprise OID value should be given in angular brackets like **<.1.3.6.1.2.1.11>**. In this case, only the trap with this OID will be matched. If the value is given as *, then all the OID's will be matched. The enterprise field should not be left empty.
Generic Type	Each SNMP v1 trap has a Generic type number. This number can used for specifying the match criteria. You can specify the Generic Type (GT) number in this field, so that the trap parsers will be applied if the incoming trap has a GT value equal to the one specified in this field.
Specific Type	Each SNMP v1 trap has a Specific Type number as well. You can also use this as a match criteria for the incoming trap. When the incoming trap matches this criteria, then the trap parsers will be applied.
Severity	Severity of the resulting alarm, ranging from **info** to **Critical**.
Message	Click on the **click to Edit Message** button to type in what will appear in the text field of the alarm.
Failure Object	The most important field, it must reflect the actual problem.
Domain	The domain name for the Event.
Category	The category for a set of events or alerts.
Network	Network name associated with the event.
Node	Node value for the event.
Source	Source name for the event. If the status of the Managed Object is to be updated with the severity of the event, the Source should match the Managed Object name.
Group Name	The group name if alarms or events are to be grouped.
Help URL	The help file, which is this document.
More	After selecting this button you can include additional properties for the Event. This is explained in more detail below.
Add Trap Parser	Create a new trap parser with all fields editable. The **Update** button adds it to the Trap Parser list. If all of the fields are the same as an existing Trap Parser, an error message appears. If the name you choose already exists in a file (config directory) or the MIB (mibs directory), an error message appears.
Modify Trap Parser	Change an already existing trap parser.
Delete Trap Parser	Delete the selected trap parser. If the parser exists in the config or mibs directory, it will be deleted from the directory.
Update	Update the modified trap parser. The change will not take effect until the Apply to Server button is selected.

TABLE 27-2 Trap Parser Configuration Form

Option	Description
Apply to Server	Make the changes permanent.
Load from MIB	Loads the trap file from the mibs directory so the traps can translated to a trap parser. This is explained in more detail below.
Load from File	Loads the trap file from the conf directory. This is explained in more detail below.
Save to File	Brings up the **Save <type of information> to File** form. Save the trap parsers as a file. The default path is to the `conf` directory. This allows the configured trap parser to be used again and as a backup. *Note: When saving these files, the AlliedView NMS sets as the default directory the* `<AlliedView NMS Home>/state` *directory, so for example the file path:* ../conf/trap.parsers *is being saved in the* `conf` *directory by going up one level from the* `state` *directory (..) and then down to the* `conf` *directory. If the user enters in the form only a file name, that file is being saved in the default* `state` *directory.*
Cancel	Cancels the update.
Help	Brings up this section of this document.
Close	Closes the form. If no changes were applied to the server, they are lost. If changes have been made, there is a prompt on whether to apply the changes.

27.3.1 Using Trap Values in the PDU

To help define the values for the event output, tokens are available in the incoming trap PDU. These can be used when defining the output values for the trap parser. These are listed in the following table.

TABLE 27-3 Tokens to Access the Properties of the Trap PDU

Token	Description
$Agent	**SNMP V1 Traps:** If the device corresponding to the agent address returned by the trap has already been discovered by Web NMS, then this token will fetch the name of the parent Managed Object, corresponding to the interface object matching the agent address of the trap received. If the device corresponding to the agent address of the trap has not been discovered, then this token will return the corresponding IP address of the agent address from which the trap has been received. For example, if a trap is received from an agent and if the corresponding device has already been discovered by AlliedView NMS, then the interface object will be IF-web server and the name of the parent managed object will be web server. In this scenario, $Agentwill return webserver. In case the device is not yet discovered, then $Agent will return the IP address (192.168.1.30.). **SNMP V2c & v3 Traps:** If the device corresponding to the source address contained by the trap received has already being discovered by AlliedView NMS, then this token will fetch the name of the parent Managed Object, corresponding to the interface object matching the source address of the received trap. If the device corresponding to the source address of the trap has not yet been discovered, then this token will return the IPaddress of the Source of the Trap.
$Community	This token will be replaced by the community string of the received trap.

TABLE 27-3 Tokens to Access the Properties of the Trap PDU (Continued)

Token	Description
$Enterprise	This token will be replaced by the enterprise id of the received trap. Applicable only in the case of SNMP traps, or else replaced with a blank.
$GenericTyp e	This token will be replaced by the generic type of the received trap. Applicable only in the case of SNMP v1 traps, or else replaced with a blank.
$Source	If the device corresponding to the source address contained by the trap received, has already been discovered by AlliedView NMS, then this token will fetch the name of the parentManaged object, corresponding to the interface object matching the source address of the received trap. If the device corresponding to the source address of the trap received has not yet been discovered then the corresponding IP address of the source address will be returned.
$SpecificType	This token will be replaced by the specific type of the received trap. Applicable only in the case of SNMP v1 traps, or else replaced with a blank.
$Uptime	This token will be replaced by the uptime value in the received trap.
$TrapOID	This token will be replaced by the trap OID of the received trap. Applicable only in the case of SNMP v2C traps, or else replaced with a blank.
$*	This token will be replaced by all the variable bindings (both OID and variable values) of the received trap. for example, for the following varbinds, 2.2.1.1.221 INTEGER 30 .1.3.6.1.2.1.1.1 STRING abc 2.2.1.1.1 INTEGER 10 the result will be: **ifIndex: 30, sysDescr: abc, ifIndex: 10**
$#	This token will be replaced by all the variable binding values (only variable values and not OIDs) of the received trap. For example, for the following varbinds, 2.2.1.1.221 INTEGER 30 .1.3.6.1.2.1.1.1 STRING abc 2.2.1.1.1 INTEGER 10 the result will be: **30, abc, 10**
$N	Here N is a non-negative integer. This token will be replaced by the (N+1)th SNMPvariable value in the variable bindings of the received trap. The Index N starts from 0. For example, for the following varbinds, 2.2.1.1.221 INTEGER 30 .1.3.6.1.2.1.1.1 STRING abc 2.2.1.1.1 INTEGER 10 and for **%1**, the result will be: **abc**
@*	This token will be replaced by all the OID labels in the variable bindings of the received trap. Example: For the following varbinds, 2.2.1.1.221 INTEGER 30 .1.3.6.1.2.1.1.1 STRING abc 2.2.1.1.1 INTEGER 10 the result will be: **ifIndex: sysDescr: ifIndex**
@N	This token will be replaced by the (N+1)th OID value in the variable bindings of the received trap. The index count starts from 0. This token will be replaced by the (N+1)thOID label in the variable bindings of the received trap. The index starts from 0. For example, for the following varbinds, 2.2.1.1.221 INTEGER 30 .1.3.6.1.2.1.1.1 STRING abc 2.2.1.1.1 INTEGER 10 and for **@1**, the result will be: **sysDescr**
$IP-Source	This token will be replaced by the IP address corresponding to the source address of the trap received.
$IP-Agent	This token will be replaced by the IP address corresponding to the agent address of the trap received.
Special Purpose Tokens - The associated Managed object should have been discovered already by Web NMS for using the following special purpose tags (or tokens). This is applicable for all special purpose tags (or tokens) listed in this section.	

TABLE 27-3 Tokens to Access the Properties of the Trap PDU (Continued)

Token	Description
$AgentMO	This tag (or token) facilitates the accessing of managed object properties.The tag can be used to access any properties of the Parent managed object for the interface object corresponding to the agent address of the received trap. (Fetching the Managed Object is similar to the $Agent tag mechanism). For example, if the user wants to access the "pollInterval" property of the Parent Managed object corresponding to the agent address of the received trap and then assign it to some property of the Eventobject generated, the user should specify the tag as $AgentMO(pollInterval) against the specific property of the Event. **Usage:-** $AgentMO(PropertyName)
$IF-AgentMO	This tag is similar to $AgentMO, except that the properties of the interface managed object's corresponding agent address of the received trap could be accessed using this tag. In the case of SNMP V2c traps, it will be exactly the same as $IF-SourceMO. **Usage:-** $IF-AgentMO(PropertyName)
$IF-Agent	This is similar to $Agent, except for that it results in the interface managed object name corresponding to the agent address of the trap received. In the case of SNMP V2c traps, it will be exactly the same as $IF-Source. **Usage:-** $IF-Agent
$SourceMO	The tag can be used to access any properties of the Parent managed object for the interface object corresponding to the source address of the received trap. (Fetching the Managed Object is similar to the $Source tag mechanism). For example, if the user wants to access the "pollInterval" property of the Parent Managed object corresponding to the source address of the received trap, in order to assign it to some property of the Event, the user has to specify the tag as $SourceMO(pollInterval) against the specific property of the Event. **Usage:-** $SourceMO(PropertyName)
$IF-SourceMO	This tag is similar to $SourceMO, except that the properties of the interface managed object corresponding to the source address of the received trap could be accessed using this tag. **Usage:-** $IF-SourceMO(PropertyName)
$IF-Source	This is similar to $Source, except that it results in the interface object name corresponding to the source address of the trap received. **Usage:-** $IF-Source

27.3.2 Loading from a MIB

To load a MIB with defined traps that can then be translated to trap parsers, click **Add Trap Parser,** and then click **Load from MIB**. A dialog box prompts for the filename of the MIB.

The filename path should be relative to the <Web NMS Home>/servlets directory. If the MIB depends on (imports) other MIB files, they should be listed in order, separated by spaces.

For example, if A-MIB imports B-MIB imports C-MIB (all files in the <Web NMS Home>/mis directory, then enter the following:

Input: ../mibs/C-MIB ../mibs/B-MIB ../mibs/A-MIB

The trap parsers are created only from the last MIB file. Clicking **Create Parsers** will load the MIBs and create trap parsers from the last file. You can then set the event object fields for the created parsers. If no severities are specified, the default **Info** will be used.

27.3.3 Loading from a File

To load a set of trap parsers previously saved by the **Save to File** button and add them to the list of Trap Parsers, click **Load From File,** and in the dialog box, enter the filename on the server that contains the trap parsers. The trap parsers are usually stored in `<Web NMS Home>/conf/trap.parsers`. Clicking **Load** will load the trap parsers from the file. Parsers with the same matching criteria are replaced. If the Trap Parser name is the same, there is confirmation prompt to replace the existing one. Once loaded, the **Apply to Server** button makes the changes permanent. The trap parsers in the `trap.parsers` file will load the next time the AlliedView NMS server starts.

27.3.4 Reordering the Trap Parser List

The list for Trap Parsers is in the order the AlliedView NMS tries to find a match. To reorder the list, select a Trap Parser and drag it up or down the list.

27.4 Configuring Event Parsers

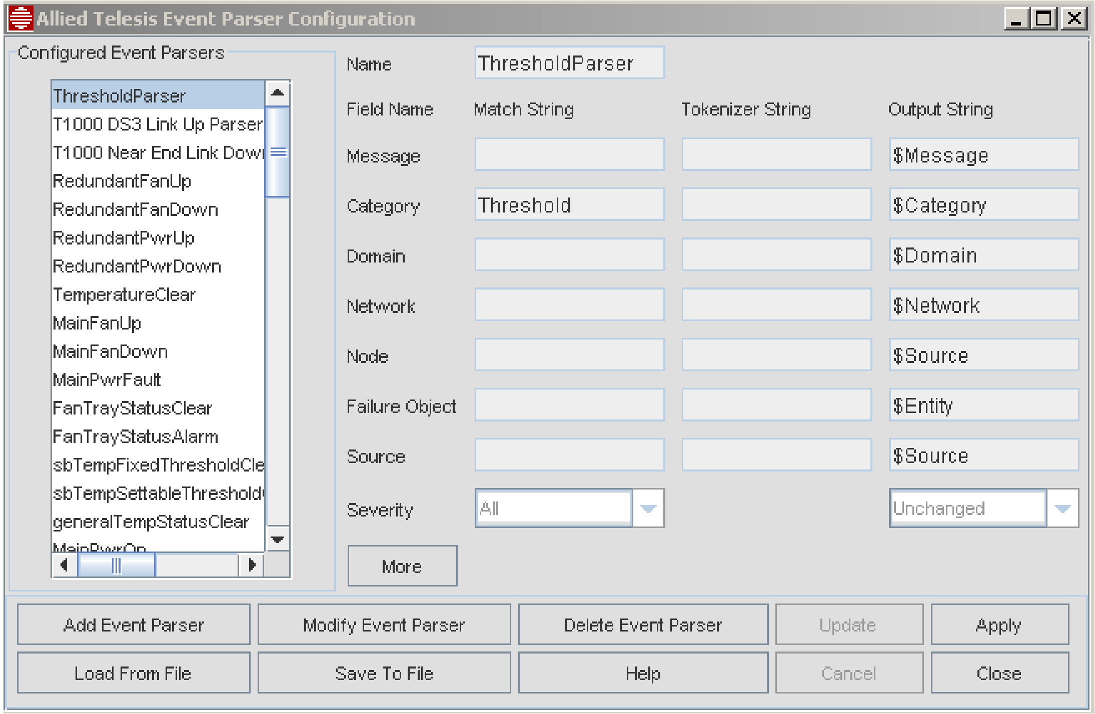
When an event arrives into the AlliedView NMS, the event parsers list is checked to see whether the incoming event satisfies the match criteria of the event parser. If the event parser matches, the event is passed through the corresponding event parser. The outgoing event from the parser is then matched with the remaining set of parsers (if any, in sequence). If there are any matches, then the event will be passed through those parsers. This process will continue till there are no parsers left to be scanned.

In the Configured Event Parsers List, the user can view the list of currently configured event parsers. On clicking any of them, the corresponding details will be listed. By default, the event parsers that are saved in the file **event.parsers** under `<AlliedView NMS Home>/conf` directory will be loaded automatically when the server is restarted and then displayed in the Configured Event Parsers List.

Note: *Event parsers are important to alarm correlation and should only be changed under the supervision of Allied Telesis Technical Support personnel. If you delete any of those you made degrade or destroy existing NMS functionality.*

To configure the Event parser, select *Edit -> Configure -> Event Parsers* from the main menu of the Network Events Panel.

The Event Parser Configuration form appears, as shown in the following figure.



Allied Telesis Event Parser Configuration

Configured Event Parsers

ThresholdParser
T1000 DS3 Link Up Parser
T1000 Near End Link Dowi
RedundantFanUp
RedundantFanDown
RedundantPwrUp
RedundantPwrDown
TemperatureClear
MainFanUp
MainFanDown
MainPwrFault
FanTrayStatusClear
FanTrayStatusAlarm
sbTempFixedThresholdCle
sbTempSettableThreshold
generalTempStatusClear
MainPwrOn

Name: ThresholdParser

Field Name	Match String	Tokenizer String	Output String
Message			$Message
Category	Threshold		$Category
Domain			$Domain
Network			$Network
Node			$Source
Failure Object			$Entity
Source			$Source
Severity	All		Unchanged

[

FIGURE 27-4 Event Parser Configuration Form

27.4.1 Setting Event Parsers

Select an Event Parser from the list to see how the fields are configured for that Event parser. The following table describes these fields at a general level, as well as the option buttons. Many of the fields will have a variable name, discussed after this table.

TABLE 27-4 Event Parser Configuration Form

Option	Description
Name	Name of the event. The name should match the type of event.
Match String	The match criteria determine whether the Event will be parsed by the given Event parser or not. If a field is left blank, it is automatically matched. Otherwise all fields (**AND** condition applied) must match the input event. To specify a match criteria, the following may be used in expressions. **Wild Card - Asterisk (*):** To signify match 0 or more characters of any value. e.g., *Failed* will match any String with *Failed* somewhere in it. **Negation - Exclamation (!):** This can be used at the start of a field, to specify exclusion of Events matching the succeeding expression. e.g., !Failed will exclude Strings with Failed anywhere in them. *Note: Expressions like *Failed, Fai*d and * have the expected meanings in the match criteria.*
Tokenizer String	Allows you to break up the input field into a series of tokens that can then be used in the output Event object. The tokenizer definition is a string with the tokens represented by $1, $2, etc. Only positive integers are allowed following '**$**'. Example: Consider the case, where you expect an event message text string as: *Line Card 31 failed on Shelf 54: No Response* - (Match String). The Line Card Number (31) and the Shelf Number (54) may be required while defining other properties of event, so they will be tagged as tokens with a token number. *Line Card $1 failed on Shelf $2: No Response* - (Tokenizer String). After such tokenization, the token number is used in the output event definition. Specifying $text$1 for any field in the output event definition will be replaced with the value 31, while specifying $text$2 will be replaced with 54. *Note: To identify the Replaceable parameter of a specific field, the token number should be preceded by the field, for example $text$1 indicates the first tokenized string of the field Message.* The tokens of any field can be used in any other field, provided this Note is followed.

TABLE 27-4 Event Parser Configuration Form (Continued)

Option	Description
Output String	The output of the event parser is an Event object, which will be the modified instance of the incoming event. The attributes of the Event object are defined by what are specified in the event parser, so it is necessary to select correct values for important attributes such as failure object (affected Entity), severity, and message text. The properties that should remain unchanged must be specifically noted by placing a dollar followed by that property name. For example, if the *text* field should not be modified, then the value *$text* should be entered in the Output String. When specifying the output values in the definition column, to use the values of the incoming event properties, you should specify the exact property name (case sensitive) with a prepended **$.** For example to use the event property *source,* the definition should be *$source*. If the particular property has been tokenized and if user intends to use the value of the token, then the format should be **$propertyname$N**, where **N** should be the count of the token starting with 1. When it is necessary to deliberately have a null value for a specific property of the Output Event, then the Output String for that property should be left blank. The default properties of event that can be used in the definition column following **$** are: *category, domain, entity, groupName, helpURL, network, node, source, severity, text, WebNMS*. Apart from the listed default properties of the event, user property names can also be used. For the list of the various Event Properties and their description, refer to Event Properties.
More	Configure additional criteria based on other properties of the event, which could also include the User properties, apart from the given default set of Event properties. In the first column of the dialog, specify the "name of the property", which could be any valid property of the Event including its user property. While giving the name, ensure that the name has the same case as given in the event properties. The second column specifies the matching criteria. In the third column, user can specify the pattern in which the incoming event property has to be tokenized. The fourth column is for defining the output value of the corresponding property in the resultant event. *Note: You should note that if a criteria is configured, based on the Event user property and if no definition is given against that property, then the user property will be dropped in the resulting Event. The event properties id and time are not configurable using the event parsers. These fields will be copied to the values as that of the incoming event object.* *Note: When user properties are added to events, they can be used in additional event parsers or custom views.*
Add Event Parser	Add a new Event parser. All the fields in the screen are editable. Ensure the name is unique. If the entered name matches the existing one, then an error message will pop up with the message "**Event parser of the given name already exists. Should that be replaced?**" Clicking "**Yes**" will overwrite the existing criteria. Clicking "**No**" will quit the add operation.
Modify Event Parser	Modify an existing Event Parser. All fields are editable.
DeleteEvent Parser	Deletes the selected Event Parser. You can also click on the Event Parser and use the Del Key, or Control + Del or more than one.

TABLE 27-4 Event Parser Configuration Form (Continued)

Option	Description
Save to File	To reuse the configured event parsers and to save the event parser configuration as a backup. These files can later be loaded in to the same or another event manager. This will enable sharing of the event parser data by other users. When this option is chosen, a dialog window will be brought which will prompt you to enter a filename (the default being event.parsers). Enter the name of the file and choose Save option to save the trap parser. When saving these files, the AlliedView NMS sets as the default directory the `<NMS Home>/state` directory, so for example the file path: ../conf/event.parsers is being saved in the `conf` directory by going up one level from the `state` directory (..) and then down to the `conf` directory. If the user enters in the form only a file name, that file is being saved in the default `state` directory.
Load from File	To load a set of event parsers previously saved with the **Save To File** option and add them to the existing list of event parsers. This option brings up a dialog box to specify the filename on the server, which contains the event parsers. Choosing the **Load** option will complete loading event parsers from the specified file. The parsers with the same matching criteria as that of the existing ones will be replaced with the new ones.
Update	Update the modified Event Parser. The change will not take effect until the Apply to Server button is selected.
Apply to Server	Makes and changes permanent.
Cancel	Cancels the update.
Help	Invokes this table.
Close	Closes the form. If no changes were applied to the server, they are lost. If changes have been made, there is a prompt on whether to apply the changes.

If the event object contains the trap pdu information, you can make use of the trap pdu information while defining the output events. The methodology of using the properties of the trap using symbolic notations is similar as in Trap Parsers, except for the following:.

- To access the values of the SNMP OID in the SNMP Variable bindings, the notation should start with **%** and not with **$** as in trap parser.
- To access the SNMP OID in the SNMP Variable bindings, the notation should start with **@** which is same as in trap parser.

The values of the trap pdu can be used in any of the columns, except in Tokenizer in the parser defined.

Note: If the trap pdu symbolic notation, such as %Agent, is used in the property column (while configuring Additional Criteria) when the value has also been tokenized by specifying a tokenizer string, then to refer to a token of this field use the notation as $%Agent$N, where N specifies the count of the token to be used.

27.4.2 Relationship Between User Properties and Custom Views

As explained in Table 27-4, user properties can be added using the Event Parser form and clicking the **More** button. (They can also be added by Allied Telesis software extensions.) These can then be used in additional event event parsers or custom views

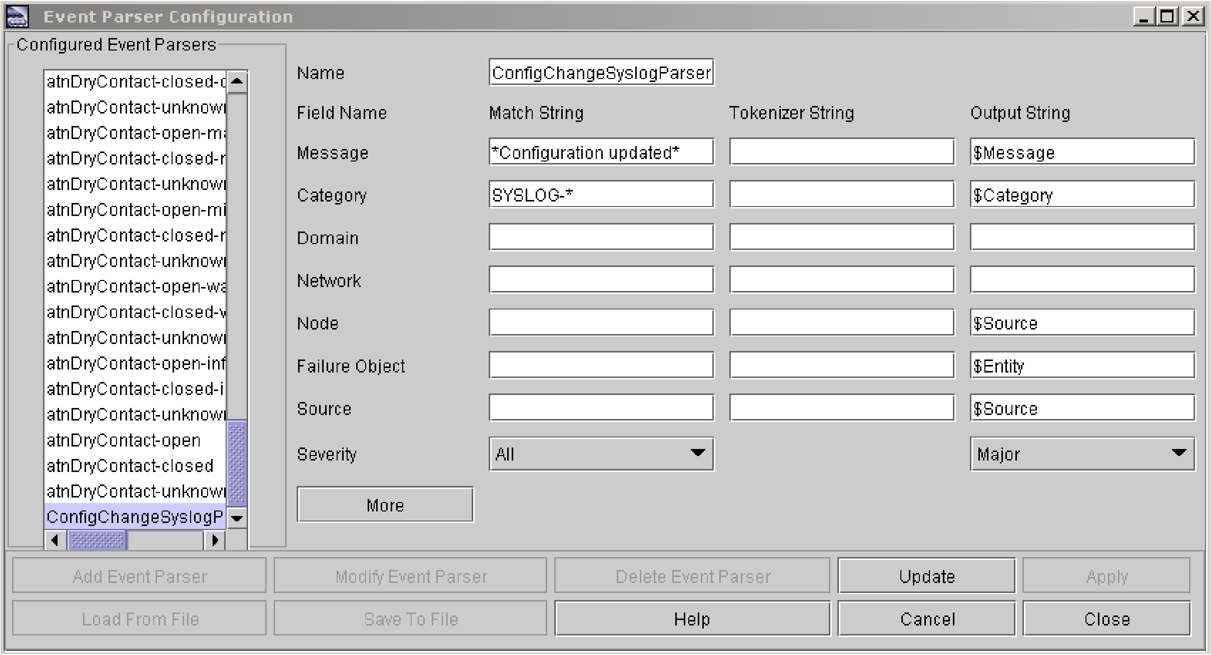
Note: When defining properties for nodes, include the properties displayed on the last page of the Managed Object Properties Form.

For Event and Alarm Custom Views, refer to Object Properties to Define Objects and Custom Views. Note that for custom alarm views only one user property, **sysLocation**, is available.

27.4.3 Setting up a SYSLOG Event to Create an Alarm

By using the Event Parser Configurator, the user can parse a SYSLOG event so that an alarm is produced. This can be useful if certain events, such as a configuration change on the a device, need to be highlighted.

Figure 27-5 shows how a SYSLOG that includes the string “Configuration Updated” can be set. The user would bring up the Event Parser Configuration window and **Add Event Parser**, in this case *ConfigChangeSyslogParser*. The Category is SYSLOG, and the Severity for the Output String is Major. (SYSLOG events have no severity level on the Match String and so the Severity is set to All.)



Event Parser Configuration

Configured Event Parsers

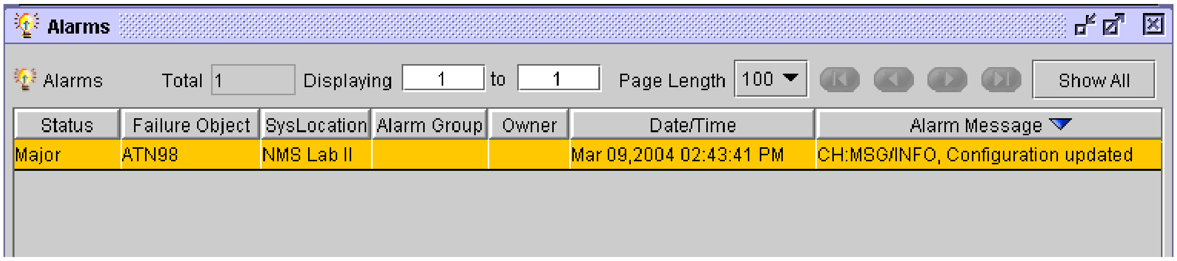
- atnDryContact-closed-c
- atnDryContact-unknowi
- atnDryContact-open-m:
- atnDryContact-closed-r
- atnDryContact-unknowi
- atnDryContact-open-mi
- atnDryContact-closed-r
- atnDryContact-unknowi
- atnDryContact-open-wa
- atnDryContact-closed-v
- atnDryContact-unknowi
- atnDryContact-open-inf
- atnDryContact-closed-i
- atnDryContact-unknowi
- atnDryContact-open
- atnDryContact-closed
- atnDryContact-unknowi
- ConfigChangeSyslogP

Name: ConfigChangeSyslogParser

Field Name	Match String	Tokenizer String	Output String
Message	*Configuration updated*		$Message
Category	SYSLOG-*		$Category
Domain			
Network			
Node			$Source
Failure Object			$Entity
Source			$Source
Severity	All		Major

FIGURE 27-5 Setting the Event Parser to Produce Alarms for SYSLOG

The usual scenario would be the device in the Physical Network view would show the device has a major alarm. Right clicking *Alarms/Events* -> *Alarms* on the affected device would show Figure 27-6. (This would also show up in the Events view as a network event.). The user could then double click the alarm row to further process the alarm, or *Edit* -> *Clear* to clear the alarm.



Alarms

Alarms Total 1 Displaying 1 to 1 Page Length 100

Status	Failure Object	SysLocation	Alarm Group	Owner	Date/Time	Alarm Message
Major	ATN98	NMS Lab II			Mar 09,2004 02:43:41 PM	CH:MSG/INFO, Configuration updated

FIGURE 27-6 Alarm Produced as a Result of Configuring Event Parser

27.4.4 Changing Severity of Default Events (i.e. Status Update Failure)

The default Event Parser Configuration Form allows the user to view and modify the events that are generated by the devices. As explained in Configuring Event Parsers, these events have attributes (especially the alarm level) that should not be changed unless with consultation with Allied Telesis personnel.

For default events (such as status update failure), the severity of the event is already set, but can be changed by creating an Event Parser that outputs a different Severity Alarm. Following is an overview of status update and the steps to change the severity of a status node failure from Major to Critical.

27.4.4.1 Overview

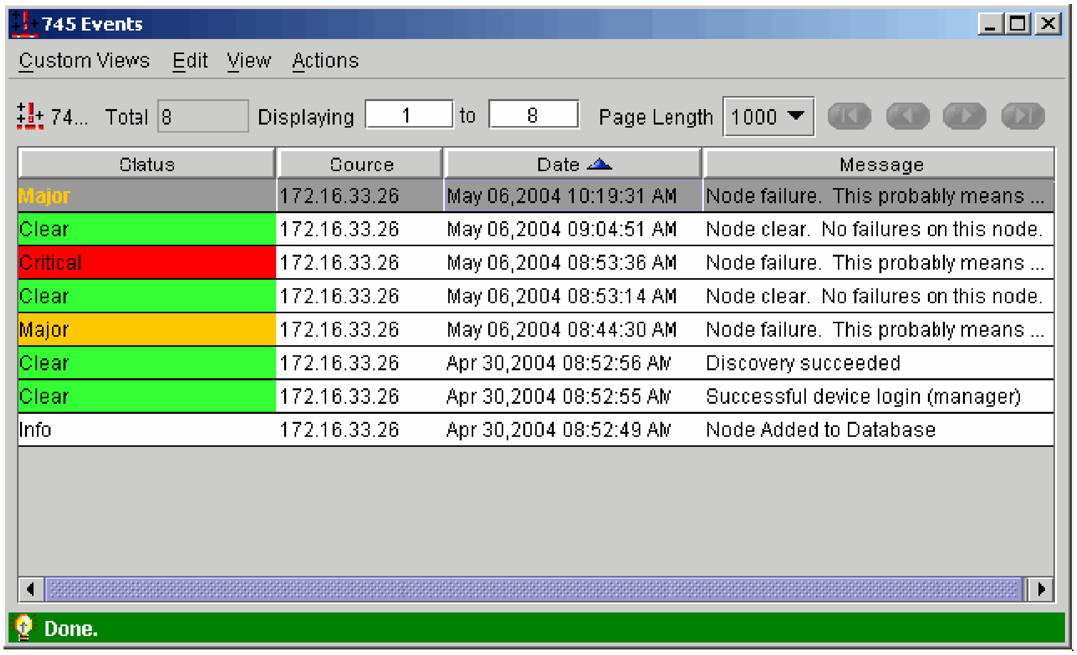
The AlliedView NMS periodically tests connectivity to all managed devices by polling their interfaces. By default, the period is 300 seconds, which can be modified with the Managed Object Properties dialogue (by changing the pollInterval parameter).

By default, when connectivity is lost a major event is created, which in turn generates a major alarm. This example shows how to make the event critical instead of major.

The process involves creating an Event Parser that examines all events, identifies the ones pertaining to lost connectivity, and changes their severity from Major to Critical.

27.4.4.2 View the Default Status Failure Event

1. Disconnect a device, which will produce the Event Node Failure.
2. Select the device and click on Update Status to force a default event to occur.
3. Go to the device's event viewer to see the list of created events. Refer to Figure 27-7.



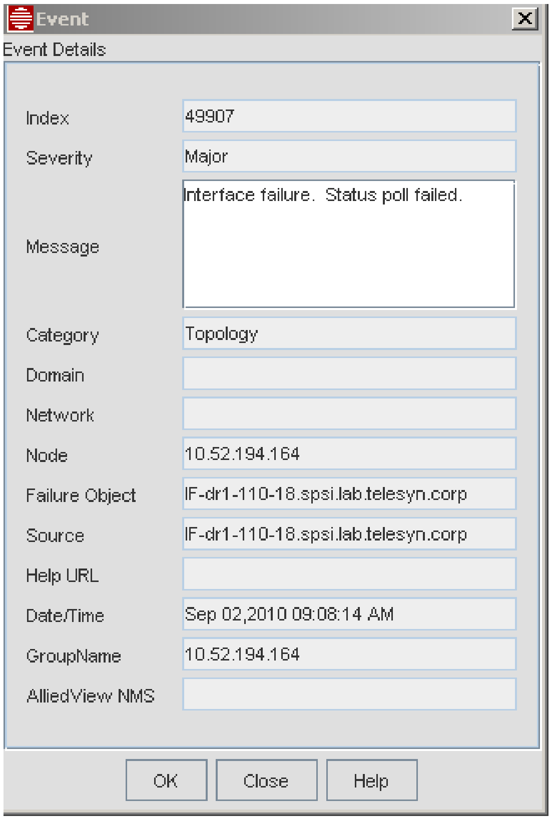
74... Total 8 Displaying 1 to 8 Page Length 1000

Status	Source	Date	Message
Major	172.16.33.26	May 06,2004 10:19:31 AM	Node failure. This probably means ...
Clear	172.16.33.26	May 06,2004 09:04:51 AM	Node clear. No failures on this node.
Critical	172.16.33.26	May 06,2004 08:53:36 AM	Node failure. This probably means ...
Clear	172.16.33.26	May 06,2004 08:53:14 AM	Node clear. No failures on this node.
Major	172.16.33.26	May 06,2004 08:44:30 AM	Node failure. This probably means ...
Clear	172.16.33.26	Apr 30,2004 08:52:56 AM	Discovery succeeded
Clear	172.16.33.26	Apr 30,2004 08:52:55 AM	Successful device login (manager)
Info	172.16.33.26	Apr 30,2004 08:52:49 AM	Node Added to Database

Done.

FIGURE 27-7 Viewing Major Level Severity for Node Failure Event

4. Double-click the major event and view its details. Refer to Figure 27-8.



Index 49907
Severity Major
Message Interface failure. Status poll failed.
Category Topology
Domain
Network
Node 10.52.194.164
Failure Object IF-dr1-110-18.spsi.lab.telesyn.corp
Source IF-dr1-110-18.spsi.lab.telesyn.corp
Help URL
Date/Time Sep 02,2010 09:08:14 AM
GroupName 10.52.194.164
AlliedView NMS

FIGURE 27-8 Viewing Object Details

5. Copy the message text (using ctl-c) so the text can be used in the new event parser to identify events of this type.

27.4.4.3 Bring up the Event Parser Configuration Dialog

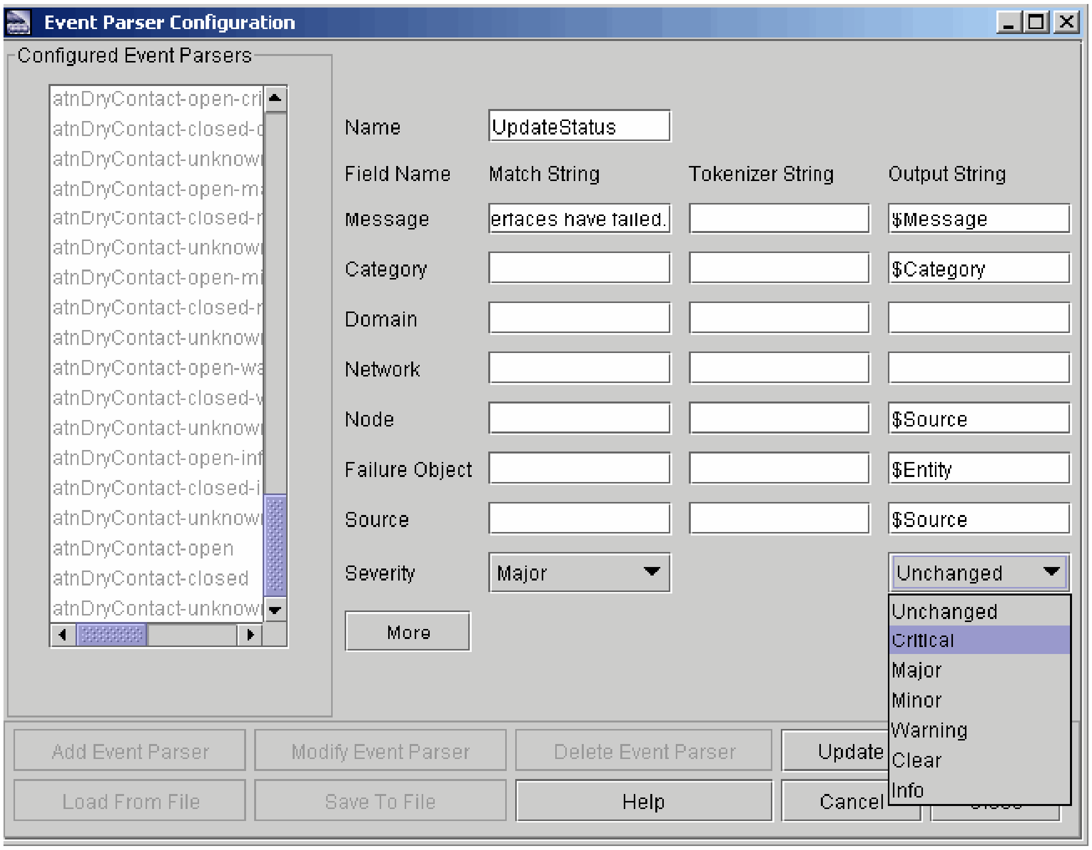
From the event browser, select **Edit -> Configure ->Event Parsers**. The Event Parser Configuration Form will appear, as was shown in Figure 27-4.

27.4.4.4 Configure the Event Parser

1. Click on Add Event Parser. The fields are now editable.
2. Give the Event Parser a name (in this example, **UpdateStatus**).
3. Enter the copied Message Text into the Message Match-String field (using ctl-v)

Note: Leave the Message Output-String unchanged if you want to use the same message or replace it with your own message text

4. Select Severity Match-String as “Major” and then Severity Output-String as “Critical”.
5. Refer to Figure 27-9, which shows the message copied in, and the Output String Severity being changed to Critical.



Name: UpdateStatus

Field Name	Match String	Tokenizer String	Output String
Message	erfaces have failed.		$Message
Category			$Category
Domain			
Network			
Node			$Source
Failure Object			$Entity
Source			$Source
Severity	Major		Unchanged

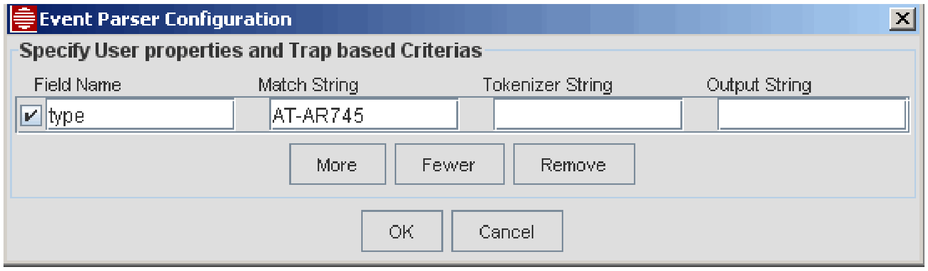
FIGURE 27-9 Creating an Event Parser and Changing the Severity

Note: *The Match Strings are used to identify which events you want to change. The Output Strings say how to change those events. In this case we're changing all those that match the existing message text exactly.*

27.4.4.5 Limit to a Specific Device Type

If you want to you can restrict this modification to one device type. In this example it will be the AT-AR745.

1. Select **More**, and enter "type" for the Field Name and "AT-AR745" for the Match String. (Device type names are available from the Manage Object Properties dialog).
2. Leave the other fields blank, as shown in Figure 27-10.


Event Parser Configuration
Specify User properties and Trap based Criterias
More
Fewer
Remove
OK
Cancel

Field Name	Match String	Tokenizer String	Output String
☑ type	AT-AR745		

FIGURE 27-10 Making an Event Parser Device Specific

3. Click on the tic box, and then OK to add the type criteria.
4. The Event Parser Configuration Form is now the only form that is on the screen. Click on **Update**, **Apply**, and **Close**.

Now only AT-AR745's when disconnected will go critical and all the others will still be major.

27.4.4.6 Ensure the Event Parser is created

1. Select **Edit -> Configure ->Event Parsers** again.
2. The Event Parser Configuration Form will appear and will include the new Event Parser.

27.4.4.7 Test the New Event Parser

1. Delete existing alarms for the device.
2. Click on Update Status, and see the color change to red, as shown in Figure 27-11.

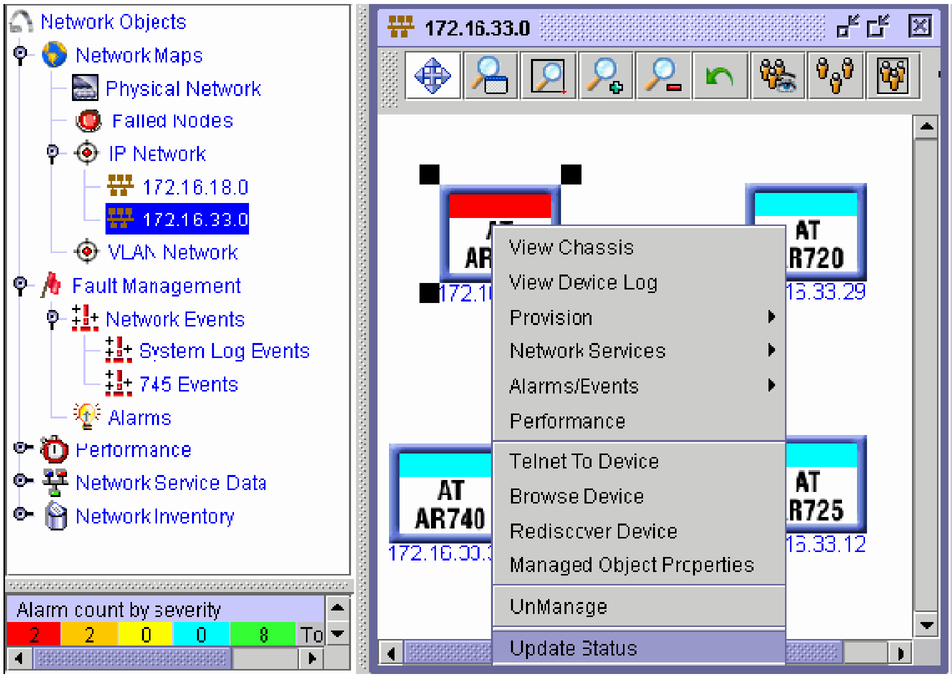


FIGURE 27-11 Testing the Changed Severity for the Event Parser (now Critical)

3. If it changed to green instead of red, either connectivity was re-established while you were creating the Event Parser, or you accidentally selected Clear on the Severity Output-String where you meant to select Critical.
4. If it goes to Orange, you misspelled the Message text, you selected Major instead of Critical, or you misspelled the type name.

Note: *A critical event will also be generated for the network to which the failed device belongs.*

27.4.4.8 Delete the Event Parser (if non-default behavior no longer needed)

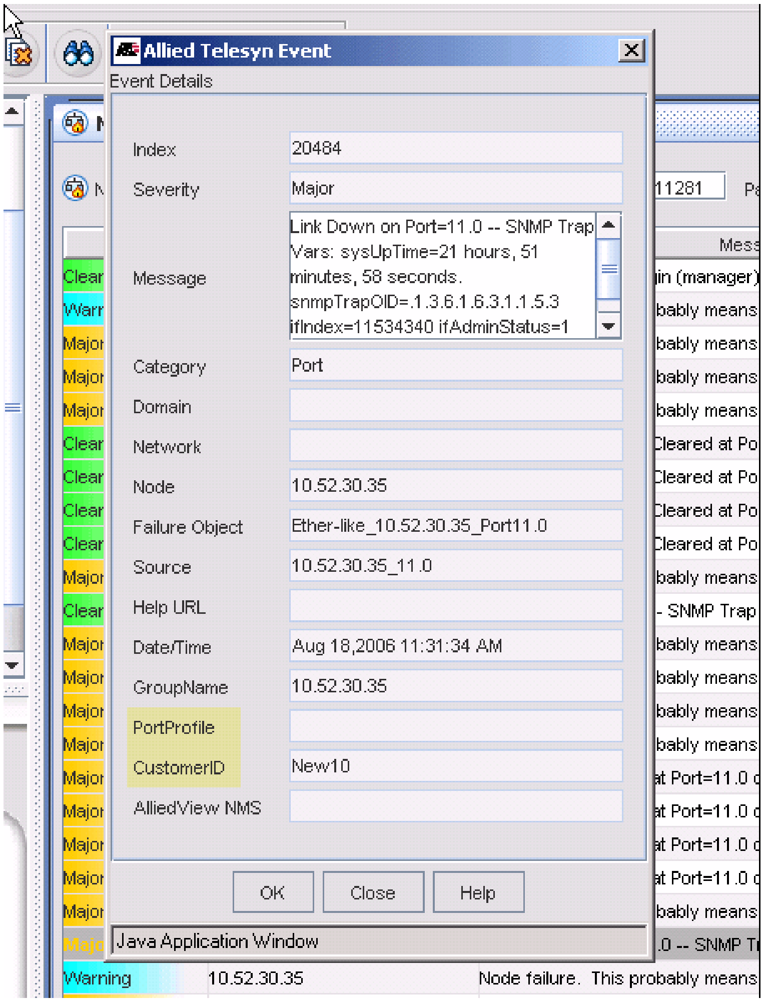
To delete the new Event Parser (and return to the default behavior), go back to the Event Parser Configuration window, select the parser you added, click on **Delete Event Parser**, **Apply**, and then **Close**.

Note: *As mentioned in Configuring Event Parsers, there are a number of pre configured event parsers already defined by AlliedView NMS. If you delete any of those you may degrade or destroy existing NMS functionality.*

27.4.5 Changing Severity of Port-based Alarms

Two attributes for the Event object are PortProfile and Customer ID. Using these attributes, the administrator can configure an Event Parser that can filter an Event that includes these attributes and changes the default priority.

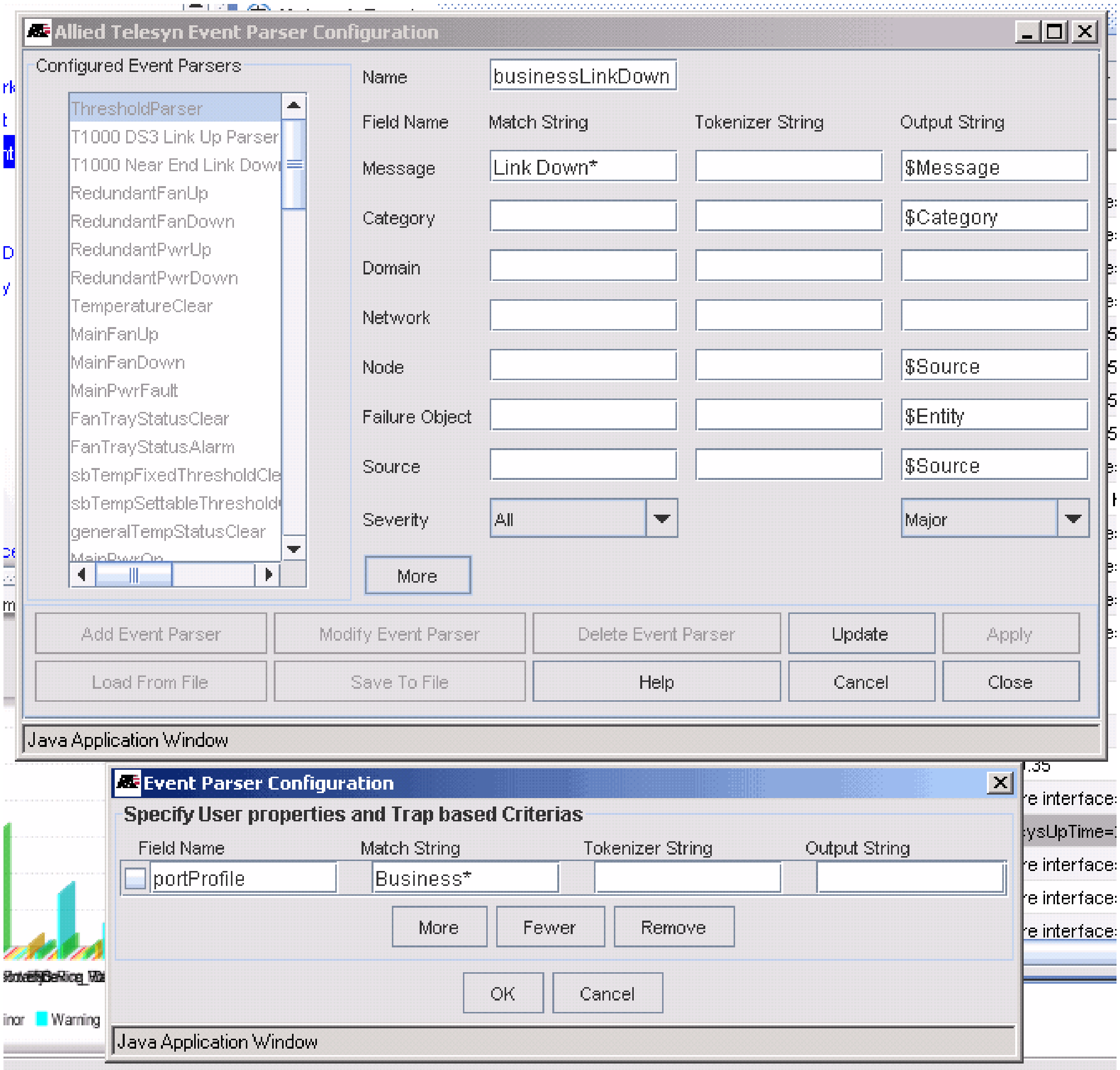
The following figure shows these two attributes that appear when the user double-clicks a port alarm and the



Index	20484
Severity	Major
Message	Link Down on Port=11.0 -- SNMP Trap Vars: sysUpTime=21 hours, 51 minutes, 58 seconds. snmpTrapOID=.1.3.6.1.6.3.1.1.5.3 ifIndex=11534340 ifAdminStatus=1
Category	Port
Domain	
Network	
Node	10.52.30.35
Failure Object	Ether-like_10.52.30.35_Port11.0
Source	10.52.30.35_11.0
Help URL	
Date/Time	Aug 18,2006 11:31:34 AM
GroupName	10.52.30.35
PortProfile	
CustomerID	New10
AlliedView NMS	

FIGURE 27-12 Object Properties for Port Alarm

By configuring the Event parser, the user can take certain events and control how they are processed, including the severity of the alarm. For example, ports can be given Profile Names that match various businesses, such as BusinessA, BusinessB, etc. In the Event Parser, Events with the Message Link Down can have a criteria set so that portProfile matches Business*. In the Output String, the Severity can be changed from Info to Major. Refer to the following figure.



Allied Telesyn Event Parser Configuration

Configured Event Parsers

ThresholdParser
T1000 DS3 Link Up Parser
T1000 Near End Link Dowi
RedundantFanUp
RedundantFanDown
RedundantPwrUp
RedundantPwrDown
TemperatureClear
MainFanUp
MainFanDown
MainPwrFault
FanTrayStatusClear
FanTrayStatusAlarm
sbTempFixedThresholdCle
sbTempSettableThreshold
generalTempStatusClear
MainPwrOn

Name: businessLinkDown

Field Name	Match String	Tokenizer String	Output String
Message	Link Down*		$Message
Category			$Category
Domain			
Network			
Node			$Source
Failure Object			$Entity
Source			$Source
Severity	All		Major

Event Parser Configuration

Specify User properties and Trap based Criterias

Field Name	Match String	Tokenizer String	Output String
□ portProfile	Business*		

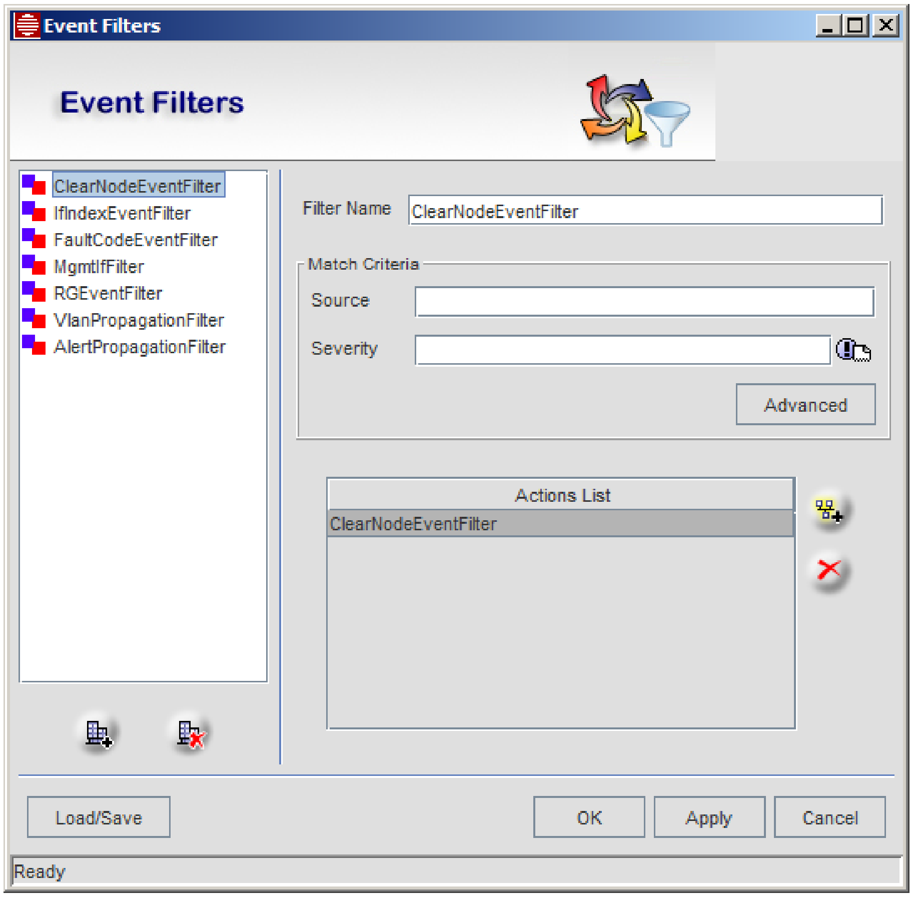
FIGURE 27-13 Configuring Event Parser with portProfile Property

27.5 Configuring Event Filters

Event filters allow you to set matching criteria to filter events and configure an action (such as an email) for these events.

To create an event filter with an associated event filter action:

1. In the **Network Objects** panel, go to **Fault Management** > **Network Events**.
2. From the menu, go to **Edit** > **Configure** > **Event Filters**. The **Event Filters** screen appears.



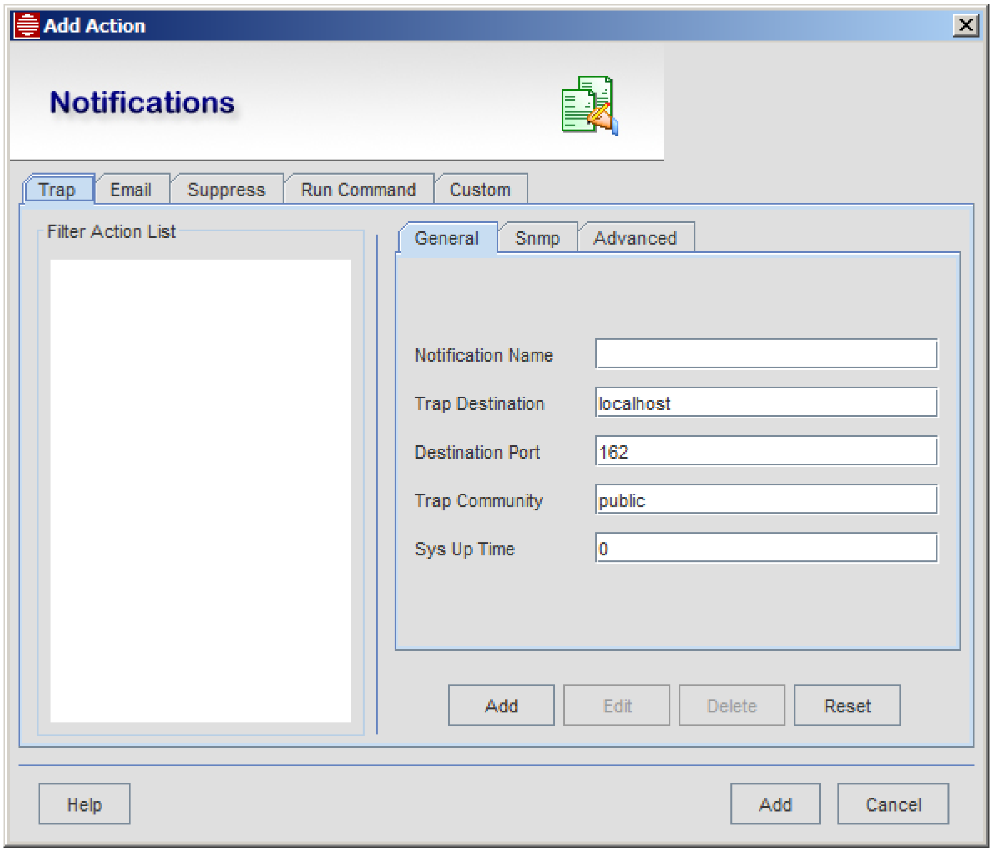
- ClearNodeEventFilter
- IfIndexEventFilter
- FaultCodeEventFilter
- MgmtIfFilter
- RGEventFilter
- VlanPropagationFilter
- AlertPropagationFilter

Filter Name: ClearNodeEventFilter

Actions List
ClearNodeEventFilter

FIGURE 27-14 Event Filters

3. Click to add an event filter.
4. In the **Filter Name** field, enter a name for the event filter.
5. Under **Match Criteria**, enter the match criteria to use for the event. See Event Filters for information on each criteria. Click **Advanced** to see additional criteria.
6. Click to add an action. The **Add Action** screen appears.



Notification Name:
Trap Destination: localhost
Destination Port: 162
Trap Community: public
Sys Up Time: 0

FIGURE 27-15

7. Select the tab for the action type you want to add. See Event Filter Actions for information on each action type.

Note: *The fields on the Advanced tab are required for every Trap, Email and Run Command event filter action, including existing event filters carried over from previous versions of the NMS. The tables in Event Filter Actions identify the values you need to enter in the Advanced tab fields.*

8. Click the top **Add** button to add the action to the Filter Action List.
9. To add another action, click **Reset**.
10. Click the bottom **Add** button to add the action
11. In the **Event Filters** screen, click **OK**.

Note: *You must restart the NMS server for changes to take effect.*

27.5.1 Event Filters

The following matching criteria are available:

TABLE 27-5 Event Filters

Option	Description / Fields
Filter Name	Name of the filter. This field matches the filter chosen in the Configured Filter List.
Match Criteria	The criteria for the event are as follows: • **Source** - Holds the information about the source of the event. Events matching a source can be filtered out using this field. • **Severity** - Specifies the match criteria based on the severity of the event (Critical, Major, etc.). Click **Advanced** for additional filter criteria: • **Message** - The message specified in this field will be matched with the message of the incoming event (Interface failure, Status Poll failed, etc.). • **Category** - This is a property of the event object which could hold a category name to which the event belongs. This is used for better organization of events. • **Domain** - This is a property of the event object which could hold any domain-specific information. The information may either be based upon the physical location or the functional / logical categorization of the source of the event. The domain name of the event can be specified to display events of a particular domain. • **Network** - Holds the information about the network to which the source of the event belongs. Using this criteria, events belonging to a particular network can be displayed. • **Node** - Holds any additional information about the source of the event. Event filters can be specified for events that have the name of the node as specified in this field. • **Entity** - Stores information about the exact device in which the problem has occurred.

TABLE 27-5 Event Filters (Continued)

Option	Description / Fields
Setting Match Criteria	Determines whether the incoming event should be filtered or not. If a field is left blank, it is automatically matched. The condition for the event filter to be applied is that all the match criteria specified should be satisfied. If one criteria fails, the filter will not be applied. You can use the following expressions to specify match criteria: • **Wildcard - Asterisk (*):** A match of 0 or more characters of any value. • For example, “**Failed***” will match any string starting with **Failed**. Expressions like ***Failed**, **Fai*led***, or * can be used which have relevant meaning. • **Negation - Exclamation (!):** Used at the start of the field to specify exclusion of events matching this expression. For example, **!Failed** will exclude strings starting with “Failed”. • **Separator - Comma (,):** Multiple values can be specified for a single match criteria for separating them with commas (a logical OR). For example, **Critical, Major** will match a string which is either Critical or Major. For another example, if all the objects with names starting with "abc" or "xyz" are required, then property key -name and value **abc*,xyz*** is given • **Comma (,) with !:** When used together, this will match the string by using a logical AND. For example, the property key-name of ***xyz,!abc*** must match all names that end in xyz AND begin with abc. • **&& (Double Ampersands):** This is also used for searching objects where a single value should be matched with many patterns. For example, if all the objects with names starting with either "abc" or ending with "xyz" are required, then property key -name and value **abc*&&*xyz** is given. • \ **(Back Slash)**: This is used when the name of the object itself contains a comma. This character is called an escape sequence, since it avoids searching of the objects, as if it were two different names. For example, if an object with name "a,b" has to be searched, then the property key - name and the value **a\,b** is given. • **<between>"value1" and "value2":** This is used to get objects with some numeric values within a specific range. For example, if object names with poll interval value ranging from 300 to 305 is required, then the property key - pollinterval and the value as 300 and 305 is given. Note that the first number is smaller than the second number. Only the values in between the given values, including the limits, will be matched.
More Properties	Allows you to add additional properties not available in the Match Criteria user interface. For information on adding properties and creating custom views, see Object Properties to Define Objects and Custom Views.
Add Filter	Adds a new event filter.
Delete Filter	Deletes the selected event filter.
Load/Save	Loads or saves a set of filters from/to a file. When you save a file, the default directory is the <NMS Home>/state directory.

27.5.2 Event Filter Actions

You must associate at least one action with each event filter. The following action types are available:

- **Trap**: Send SNMP V1 and V2 traps for events matching particular filter criteria.
- **Email**: Send an email for events matching particular filter criteria.

- **Suppress**: Suppress events that match the filter criteria. You can suppress all events or multiple events of the same type within a given interval.
- **Run Command**: Run a command on the server for events matching particular filter criteria. Commands can be used to send a page to someone, email or any other desired command.
- **Custom**: Write your own Java code to filter events and perform actions based on filter criteria.

Tips to keep in mind when creating event filter actions:

- The fields on the **Advanced** tab are required for every Trap, Email and Run Command event filter action, including existing event filters carried over from previous versions of the NMS. The tables below identify the values you need to enter in these fields.
- After you create or modify an event filter, you must restart the NMS server for the changes to take effect.

The following tables list the fields available for each action type.

27.5.2.1 Trap Actions

TABLE 27-6 Fields for Trap Actions

Tab or Box	Field	Description
General	Notification Name	Name of this action required for identification
	Trap Destination	This is used to specify the hostname (IP address) of the host to which the SNMP trap will be sent.
	Destination Port	The port to which the trap is to be sent.
	Trap Community	This specifies the community string of the generated SNMP trap.
	SysUpTime	The time, in seconds, since the last system restart.
SNMP	SNMP Version	V1 or V2C.
	Enterprise	Specifies the enterprise OID of the generated SNMP trap.
	Generic Type	Used to specify the generic type number for the trap to be generated.
	Specific Type	Used to specify the specific type number for the trap to be generated.
Variable Binding List	List	A listing of the bound SNMP variables. Click **List** for the Variable Binding List box.
	OID Value	Enabled when Add is selected.
	SNMP Type	The SNMP variable type (STRING, IPADDRESS, OPAQUE, OBJID, INTEGER, GUAGE, COUNTER, or TIMETICKS).
	Set Value	The value to which the variable is to be set.
Advanced NOTE: ALL FIELDS ON THIS TAB ARE REQUIRED.	Handler Impl For Events	The class that handles trap notification for event processing. The value to enter is: **com.adventnet.nms.eventdb.SendTrapEventAction**.
	Handler Impl For Alerts	The class that handles trap notification for alert processing. The value to enter is: **com.adventnet.nms.eventdb.SendTrapAlertAction**.
	Add, Edit, Delete, Reset	Add - Add the new filter action to the Filter Action List Edit - Save modifications to the selected filter action. Delete - Delete the selected filter action. Reset - Resets the fields to allow you to add a new filter action.
	Add	Add - Add the filter action to the event filter's Action List.

27.5.2.2 Email Actions

TABLE 27-7 Fields for Email Actions

Tab	Field	Description
General	Notification Name	A name to identify this action.
	SMTP Account	The SMTP account that will send the email. Select the account from the drop-down list or click **Configure** to create a new account.
	Subject	Subject of the email. This can use variables ($) from the Filter Name if they have been specified.
	Message	Text of the email message. This can use variables ($) from the Filter Name if they have been specified.

TABLE 27-7 Fields for Email Actions (Continued)

Tab	Field	Description
	File Attachment	A file to attach to the message.
Advanced NOTE: ALL FIELDS ON THIS TAB ARE REQUIRED.	Handler Impl For Events	The class that handles trap notification for event processing. The value to enter is: **com.adventnet.nms.eventdb.SendEmailEventAction**.
	Handler Impl For Alerts	The class that handles trap notification for alert processing. The value to enter is: **com.adventnet.nms.eventdb.SendEmailAlertAction**.
	Add, Edit, Delete, Reset	Add - Add the new filter action to the Filter Action List Edit - Save modifications to the selected filter action. Delete - Delete the selected filter action. Reset - Resets the fields to allow you to add a new filter action.
	Add	Add - Add the filter action to the event filter's Action List.

27.5.2.3 Suppress Actions

TABLE 27-8 Fields for Suppress Actions

Tab	Field	Description
General	Notification Name	A name to identify this action.
	Suppress All	Specifies whether all events should be suppressed or only suppress events based on interval. If 'yes' is selected then all events are suppressed and if 'no' is selected then the user will have an option to specify time interval for suppressing subsequent received events matching the same criteria.
	Suppress Interval	Used for specifying the time interval (in seconds) to suppress subsequent events.
	Add, Edit, Delete, Reset	Add - Add the new filter action to the Filter Action List Edit - Save modifications to the selected filter action. Delete - Delete the selected filter action. Reset - Resets the fields to allow you to add a new filter action.
	Add	Add - Add the filter action to the event filter's Action List.

27.5.2.4 Run Command Actions

TABLE 27-9 Fields for Run Command Actions

Tab	Field	Description
General	Notification Name	A name to identify this action.
	System Command	Specifies the actual command to be executed in the NMS server machine. The command specified here should not require a shell to run unless the shell program is specified in the command.
	append output with message	If checked, the output of the command execution is appended to the event message body.
	append error with message	If checked, command execution errors are appended to the event or alert message body. Long messages or errors are truncated.
	Abort After	Specifies the number of seconds that the command is allowed to run before command execution stops. This action can block all new events while the command is executing.
Advanced NOTE: ALL FIELDS ON THIS TAB ARE REQUIRED.	Handler Impl For Events	The class that handles trap notification for event processing. The value to enter is: **com.adventnet.nms.eventdb.FilterCommandEventAction**.
	Handler Impl For Alerts	The class that handles trap notification for alert processing. The value to enter is: **com.adventnet.nms.eventdb.FilterCommandAlertAction**.
	Add, Edit, Delete, Reset	Add - Add the new filter action to the Filter Action List Edit - Save modifications to the selected filter action. Delete - Delete the selected filter action. Reset - Resets the fields to allow you to add a new filter action.
	Add	Add - Add the filter action to the event filter's Action List.

27.5.2.5 Custom Actions

TABLE 27-10 Fields for Custom Actions

Tab	Filter Action Detail	Description
Custom	Notification Name	The name of the custom filter.
	Program Name	The name of the class to which the custom filter belongs.
Advanced NOTE: ALL FIELDS ON THIS TAB ARE REQUIRED.	Handler Impl For Events	The class that handles trap notification for event processing. You must define this class.
	Handler Impl For Alerts	The class that handles trap notification for event processing. You must define this class.
	Add, Edit, Delete, Reset	Add - Add the new filter action to the Filter Action List Edit - Save modifications to the selected filter action. Delete - Delete the selected filter action. Reset - Resets the fields to allow you to add a new filter action.
	Add	Add - Add the filter action to the event filter's Action List.

27.5.3 Setting Up Event Filters for SYSLOG Events

Configuring System Logs describes how to configure system logs. To configure the event filter for system logs, you set the Category field (shown in Figure 27-17) with the string "SYSLOG-" and the Event Type. For all event types that have been configured, the string "SYSLOG-*" would be entered. You would then continue to configure the type of action.

27.6 Configuring System Logs

Logs are indications of various changes that occur in the managed devices on a network. To assist in troubleshooting network problems and in monitoring the overall health of the network, it is important to monitor certain logs as they are received from the network devices. Proper management of these system logs (also called SysLogs), is controlled by the NMS System Log Server feature, and the feature helps in monitoring and troubleshooting your network.

Up until NMS release 11.0 SP5, this feature worked as follows:

- All SysLog messages were stored in the NMS database if enabled.
- Only events that were reported by discovered devices were processed by the NMS and stored.

In NMS release 11.0 SP5, the following changes are made:

- Incoming events from **non**-discovered devices can also be received. Since the administrator may not want syslog information to be stored on the NMS database, there is also the option for SysLogs to be stored in a local file.
- The Status Monitoring GUI has a System Log tab added to the "Application Logs" option, allowing the local file to be viewed, as well as the option to export the local file to the client's browser or NMS server. Refer to Status Monitoring.

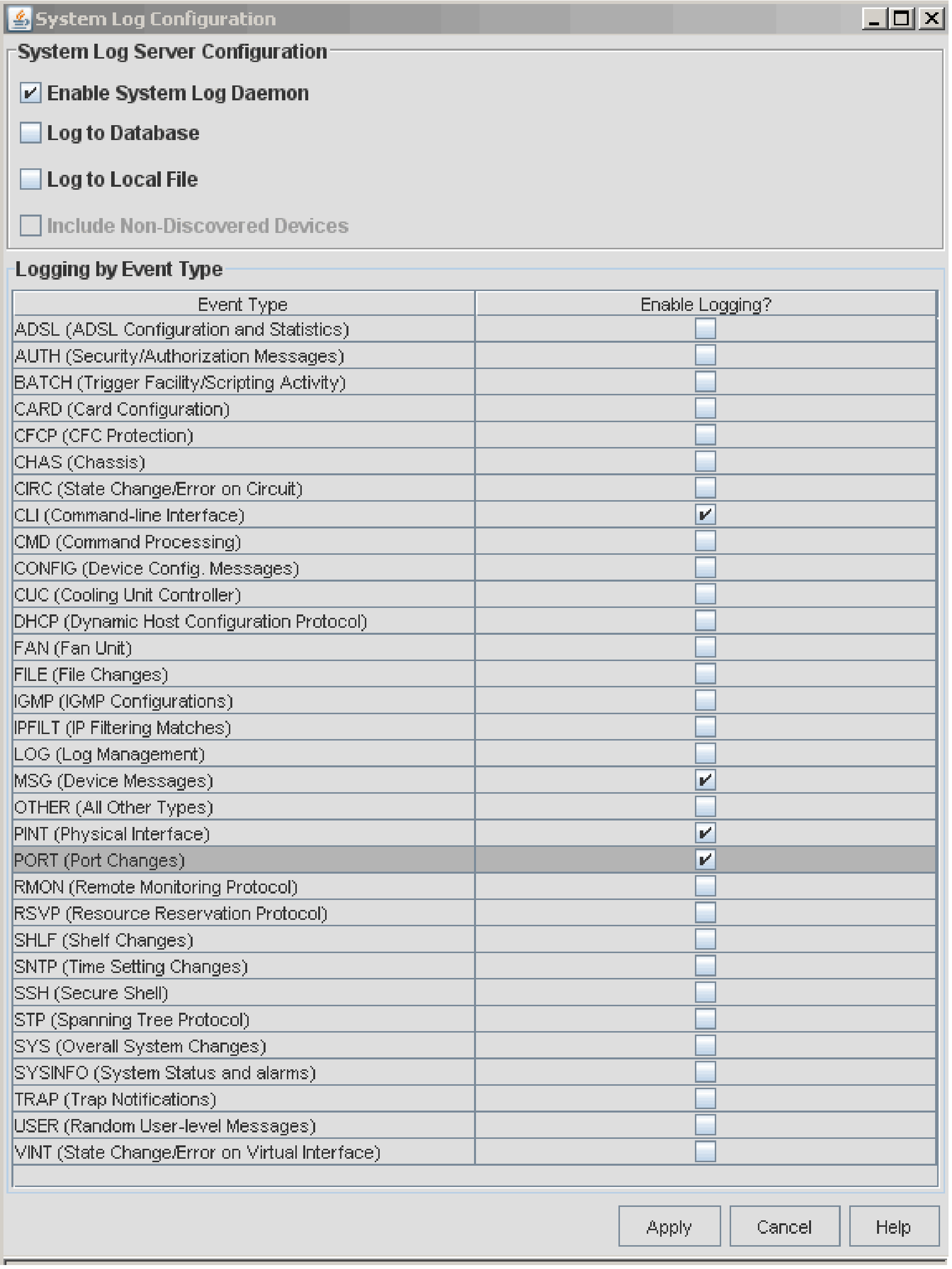
The relationship between the components that provide system logs is as follows:

- The log types that are displayed in the **System Log Events** tree node (Under **Network Events**) are those being stored in the database, and are controlled through configuring the system log server, described in Configuring the System Log Server.
- The filtering of logs produced by the device that are sent to the NMS is controlled by applying log filters. This is described in Applying Log Filters.
- Controlling what actions to take upon the reception of system logs is controlled through the Event Filter, described in Configuring Event Filters. Details on filtering for system logs are given in Setting Up Event Filters for SYSLOG Events.

Note: On Linux, upon server startup if there is a default unix syslogd running, then it will be shutdown so the port 514 is used by the NMS to run its own Syslog Process.

27.6.1 Configuring the System Log Server

The System Log Server is automatically configured to Enabled during installation. You can view the current configuration and modify it to better meet your requirements, if necessary. To view the current configuration, select *Tools* -> *System Log Configuration* for the Panel-Specific Menu. The System Log Server Configuration form, shown in the following figure, will appear.



System Log Server Configuration

☑ Enable System Log Daemon

□ Log to Database

□ Log to Local File

□ Include Non-Discovered Devices

Logging by Event Type

Event Type	Enable Logging?
ADSL (ADSL Configuration and Statistics)	□
AUTH (Security/Authorization Messages)	□
BATCH (Trigger Facility/Scripting Activity)	□
CARD (Card Configuration)	□
CFCP (CFC Protection)	□
CHAS (Chassis)	□
CIRC (State Change/Error on Circuit)	□
CLI (Command-line Interface)	☑
CMD (Command Processing)	□
CONFIG (Device Config. Messages)	□
CUC (Cooling Unit Controller)	□
DHCP (Dynamic Host Configuration Protocol)	□
FAN (Fan Unit)	□
FILE (File Changes)	□
IGMP (IGMP Configurations)	□
IPFILT (IP Filtering Matches)	□
LOG (Log Management)	□
MSG (Device Messages)	☑
OTHER (All Other Types)	□
PINT (Physical Interface)	☑
PORT (Port Changes)	☑
RMON (Remote Monitoring Protocol)	□
RSVP (Resource Reservation Protocol)	□
SHLF (Shelf Changes)	□
SNTP (Time Setting Changes)	□
SSH (Secure Shell)	□
STP (Spanning Tree Protocol)	□
SYS (Overall System Changes)	□
SYSINFO (System Status and alarms)	□
TRAP (Trap Notifications)	□
USER (Random User-level Messages)	□
VINT (State Change/Error on Virtual Interface)	□

FIGURE 27-16 System Log Server Configuration Form - Initial State

Select the checkboxes as follows:

- **Enable System Log Daemon** - Enables or disables the Log Daemon, so that events can be logged.
- **Log to Database** - Enables or disables storing of logs in the NMS database.
- **Log to Local File** - Enables or disables storing of the logs to a local file, `<NMS-Home>/logs/syslog.txt`
- **Include Non-Discovered Devices** - Enables or disables the including of system events from non-discovered devices

Note: *Various combinations of checkboxes are possible, so for example the administrator may wish to rinclude syslogs from non-discovered devices and send these only to the local file.*

- **Logging by Event Type** - a list of the types of logs that may be received from the devices. A checkbox is provided for each to allow you to enable or disable the log as needed. When checked, logs of that type are stored in the database or local file (or both) as they are received. What is selected here, as well as any log filters that are applied, control what is shown in the System Log Events table.

At the bottom of the form, the **Apply** button applies any changes you make to the form, while the **Cancel** button cancels the operation without making any changes and closes the form.

Note: *Logging a large number of event types may affect the performance of the AlliedView NMS Server. To ensure optimum performance, select only the event types that you need to monitor and disable any event types that are not needed.*

Note: *The administrator should be aware that non-discovered devices are not managed/controlled by the NMS, and are therefore not part of NMS applications.*

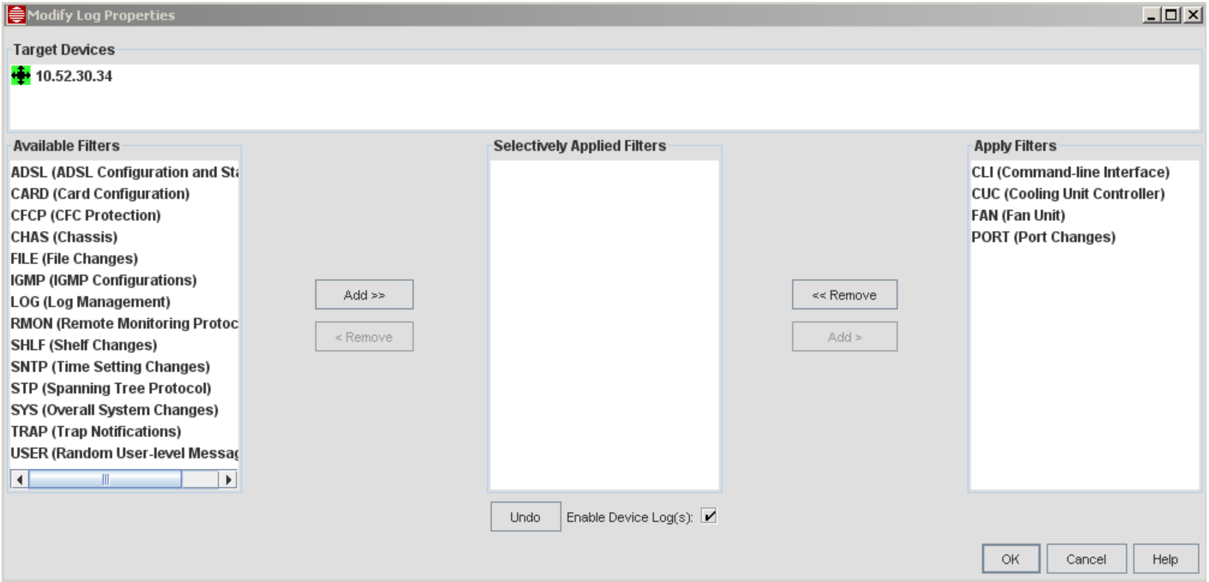
27.6.2 Applying Log Filters

You can further refine your system logging by applying log filters to your network devices on a per-device basis. Filters will screen the incoming logs and store only those of a certain type from a specific device. You can apply log filters to specific devices as follows:

1. In the NMS Tree, click the Physical Network submap under Network Maps.
2. In the Physical Network submap, select the devices on which you want to apply the log filters. (Shift+right-click to select multiple devices.)
3. In the Panel-Specific Menu Bar, select *Tools* **->** *Application Manager*.
4. From the **Application Manager** drop-down menu, select *SysLog Management*.
5. Click the **Collect Data** icon (↻) to get the latest information.
6. Select the device or devices on which you want to apply the log filters (Shift+right-click to select multiple devices), right-click, and then select *Modify Log* from the pop-up menu.

Note: *You can also select the device and click Modify.*

The Modify Log Properties form, shown in the following figure, will appear.



Target Devices

10.52.30.34

Available Filters

ADSL (ADSL Configuration and St
CARD (Card Configuration)
CFCP (CFC Protection)
CHAS (Chassis)
FILE (File Changes)
IGMP (IGMP Configurations)
LOG (Log Management)
RMON (Remote Monitoring Protoc
SHLF (Shelf Changes)
SNTP (Time Setting Changes)
STP (Spanning Tree Protocol)
SYS (Overall System Changes)
TRAP (Trap Notifications)
USER (Random User-level Messag

Selectively Applied Filters

Apply Filters

CLI (Command-line Interface)
CUC (Cooling Unit Controller)
FAN (Fan Unit)
PORT (Port Changes)

Enable Device Log(s): ☑

FIGURE 27-17 Modify Log Properties Form - File

To add a filter, select the desired filter in the **Available Filters** list, and then click **Add>>**. To remove a filter, select the filter you want to remove in the **Apply Filter**s list, and then click **<<Remove**.

Note: *Log filters are device-specific, which means a given filter may not apply to all device types. If a filter does not apply to all of the selected devices, the filter will appear in the Selectively Applied Filters list. If a filter is applied to a device that does not support the filter, the device will simply ignore the filter. When applying log filters to multiple devices, it is recommended that you select only devices of the same family.*

7. Once you have the filters you want to apply in the **Apply Filters** list, make sure the **Enable Device Log(s)** checkbox is checked, and then click **OK**.

27.6.3 Configuring Log Actions

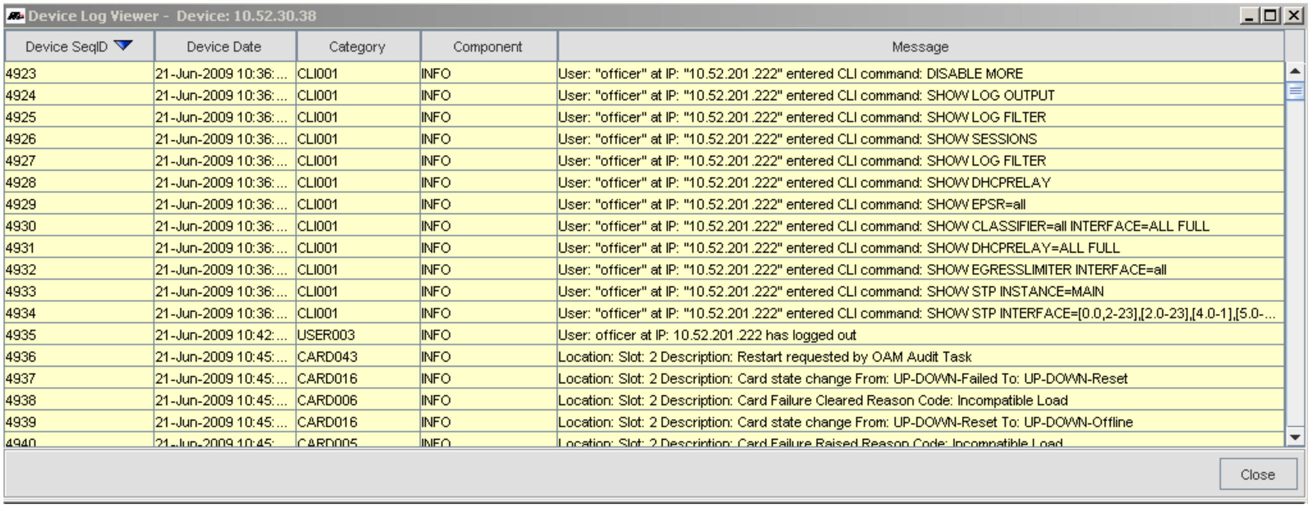
Event filters can be used to trigger actions on specific logs. The filter must specify the category of the desired log message and any other criteria applicable to the log, and an action. Refer to Configuring Event Filters for information on setting up event filters.

27.6.4 Viewing Logs

System logs are stored in the NMS database, file (or both) as they are received. The actual logs stored depend on the log types that are enabled and the log filters applied to each managed device. You can view all of the logs received on your network from the System Log Events subview of the Network Events view.

You can view logs on a specific device as follows:

1. In the NMS Tree, select the Physical Network submap under Network Maps.
2. Right-click the device on which you want to view logs, and then select **View Device Log**. The Log Management Viewer window, shown in the following figure, will appear.



Device SeqID	Device Date	Category	Component	Message
4923	21-Jun-2009 10:36:...	CLI001	INFO	User: "officer" at IP: "10.52.201.222" entered CLI command: DISABLE MORE
4924	21-Jun-2009 10:36:...	CLI001	INFO	User: "officer" at IP: "10.52.201.222" entered CLI command: SHOW LOG OUTPUT
4925	21-Jun-2009 10:36:...	CLI001	INFO	User: "officer" at IP: "10.52.201.222" entered CLI command: SHOW LOG FILTER
4926	21-Jun-2009 10:36:...	CLI001	INFO	User: "officer" at IP: "10.52.201.222" entered CLI command: SHOW SESSIONS
4927	21-Jun-2009 10:36:...	CLI001	INFO	User: "officer" at IP: "10.52.201.222" entered CLI command: SHOW LOG FILTER
4928	21-Jun-2009 10:36:...	CLI001	INFO	User: "officer" at IP: "10.52.201.222" entered CLI command: SHOW DHCPRELAY
4929	21-Jun-2009 10:36:...	CLI001	INFO	User: "officer" at IP: "10.52.201.222" entered CLI command: SHOW EPSR=all
4930	21-Jun-2009 10:36:...	CLI001	INFO	User: "officer" at IP: "10.52.201.222" entered CLI command: SHOW CLASSIFIER=all INTERFACE=ALL FULL
4931	21-Jun-2009 10:36:...	CLI001	INFO	User: "officer" at IP: "10.52.201.222" entered CLI command: SHOW DHCPRELAY=ALL FULL
4932	21-Jun-2009 10:36:...	CLI001	INFO	User: "officer" at IP: "10.52.201.222" entered CLI command: SHOW EGRESSLIMITER INTERFACE=all
4933	21-Jun-2009 10:36:...	CLI001	INFO	User: "officer" at IP: "10.52.201.222" entered CLI command: SHOW STP INSTANCE=MAIN
4934	21-Jun-2009 10:36:...	CLI001	INFO	User: "officer" at IP: "10.52.201.222" entered CLI command: SHOW STP INTERFACE=[0.0,2-23],[2.0-23],[4.0-1],[5.0-...
4935	21-Jun-2009 10:42:...	USER003	INFO	User: officer at IP: 10.52.201.222 has logged out
4936	21-Jun-2009 10:45:...	CARD043	INFO	Location: Slot: 2 Description: Restart requested by OAM Audit Task
4937	21-Jun-2009 10:45:...	CARD016	INFO	Location: Slot: 2 Description: Card state change From: UP-DOWN-Failed To: UP-DOWN-Reset
4938	21-Jun-2009 10:45:...	CARD006	INFO	Location: Slot: 2 Description: Card Failure Cleared Reason Code: Incompatible Load
4939	21-Jun-2009 10:45:...	CARD016	INFO	Location: Slot: 2 Description: Card state change From: UP-DOWN-Reset To: UP-DOWN-Offline
4940	21-Jun-2009 10:45:	CARD005	INFO	Location: Slot: 2 Description: Card Failure Raised Reason Code: Incompatible Load

FIGURE 27-18 Log Management Viewer

3. To sort the logs, click the header on which you want to sort (e.g. **Device SeqID**, **Device Date**, etc.) until the desired sort is performed (up arrow for descending or down arrow for ascending).
4. Click **Close** to close the window.

27.6.5 Disabling and Re-enabling Logs from a Device

You can disable logs from a device as follows:

1. From the Physical Network view, select the device or devices on which you want to disable logs.
2. Select *Tools* **->** *Application Manager* from the Panel-Specific Menu.
3. Select *SysLog Manager* from the Application Manager pull-down menu.

Note: For a single device, you can also access the SysLog Manager panel by right-clicking the device in the Physical Network view, and then select Provision -> Syslog Management from the pop-up menu.

4. In the **SysLog Manager** panel, select the device or devices in the list (use Shift+right-click to select multiple devices), and then click **Modify**. The Modify Log Properties form will appear as shown in Figure 27-17.
5. In the Modify Log Properties form, uncheck the **Enable Device Log(s)** checkbox, and then click **OK**. This will close the form. On the **SysLog Manager** panel, the **Status** for each selected device will change to **Disabled**. The logs for these devices are now disabled.

To re-enable disabled logs, repeat this procedure except check the **Enabled Device Logs(s)** checkbox in the last step. The **Status** for each selected device in the **SysLog Manager** panel will change to **Enabled**, which indicates that the logs are enabled for the device(s).

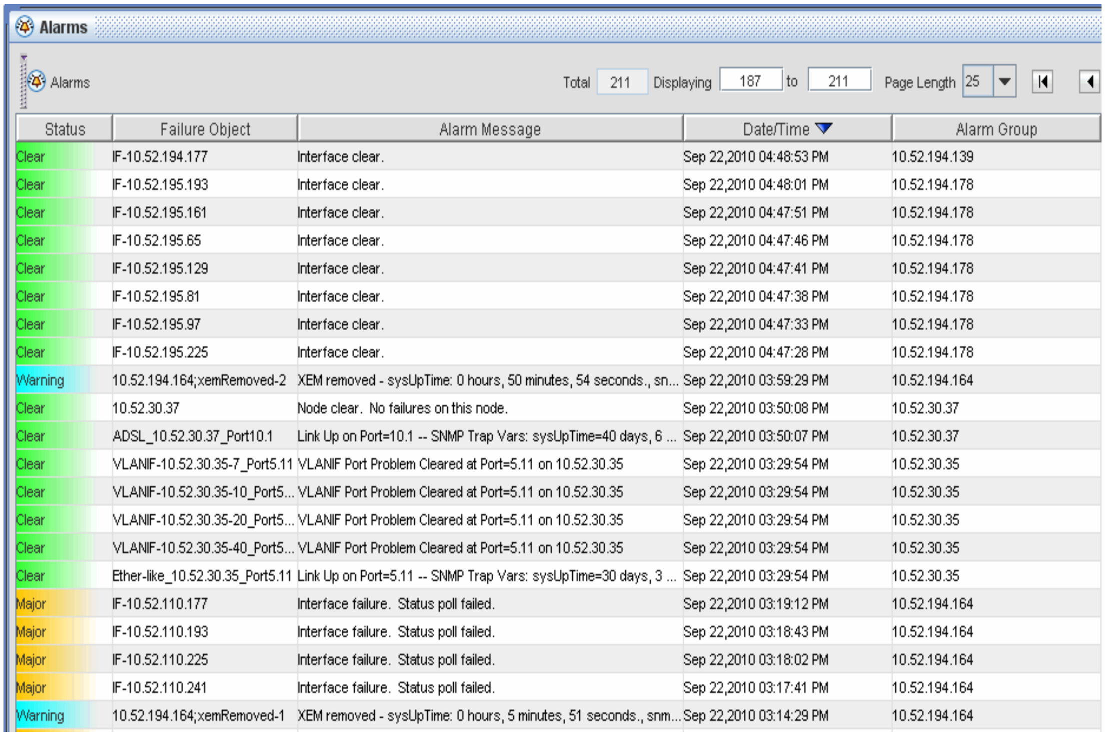
27.6.6 OTHER Event Type

An additional Event Type, OTHER, is for all other log events that are not part of the other event types. This event type can include events from debug, kernel, and third party devices.

Note: Because of the special nature of this event type, the user may find it useful to create a custom view to isolate this event type (in the Custom View form the user would fill in the Category field as SYSLOG-OTHER and then Apply Filter). This view could then be exported to a file for further analysis.

27.7 Alarm View Display

Select the node **Alarms** from the NMS Tree to view the Alarms, as shown in the following figure.



Total 211 Displaying 187 to 211 Page Length 25

Status	Failure Object	Alarm Message	Date/Time	Alarm Group
Clear	IF-10.52.194.177	Interface clear.	Sep 22,2010 04:48:53 PM	10.52.194.139
Clear	IF-10.52.195.193	Interface clear.	Sep 22,2010 04:48:01 PM	10.52.194.178
Clear	IF-10.52.195.161	Interface clear.	Sep 22,2010 04:47:51 PM	10.52.194.178
Clear	IF-10.52.195.65	Interface clear.	Sep 22,2010 04:47:46 PM	10.52.194.178
Clear	IF-10.52.195.129	Interface clear.	Sep 22,2010 04:47:41 PM	10.52.194.178
Clear	IF-10.52.195.81	Interface clear.	Sep 22,2010 04:47:38 PM	10.52.194.178
Clear	IF-10.52.195.97	Interface clear.	Sep 22,2010 04:47:33 PM	10.52.194.178
Clear	IF-10.52.195.225	Interface clear.	Sep 22,2010 04:47:28 PM	10.52.194.178
Warning	10.52.194.164;xemRemoved-2	XEM removed - sysUpTime: 0 hours, 50 minutes, 54 seconds., sn...	Sep 22,2010 03:59:29 PM	10.52.194.164
Clear	10.52.30.37	Node clear. No failures on this node.	Sep 22,2010 03:50:08 PM	10.52.30.37
Clear	ADSL_10.52.30.37_Port10.1	Link Up on Port=10.1 -- SNMP Trap Vars: sysUpTime=40 days, 6 ...	Sep 22,2010 03:50:07 PM	10.52.30.37
Clear	VLANIF-10.52.30.35-7_Port5.11	VLANIF Port Problem Cleared at Port=5.11 on 10.52.30.35	Sep 22,2010 03:29:54 PM	10.52.30.35
Clear	VLANIF-10.52.30.35-10_Port5...	VLANIF Port Problem Cleared at Port=5.11 on 10.52.30.35	Sep 22,2010 03:29:54 PM	10.52.30.35
Clear	VLANIF-10.52.30.35-20_Port5...	VLANIF Port Problem Cleared at Port=5.11 on 10.52.30.35	Sep 22,2010 03:29:54 PM	10.52.30.35
Clear	VLANIF-10.52.30.35-40_Port5...	VLANIF Port Problem Cleared at Port=5.11 on 10.52.30.35	Sep 22,2010 03:29:54 PM	10.52.30.35
Clear	Ether-like_10.52.30.35_Port5.11	Link Up on Port=5.11 -- SNMP Trap Vars: sysUpTime=30 days, 3 ...	Sep 22,2010 03:29:54 PM	10.52.30.35
Major	IF-10.52.110.177	Interface failure. Status poll failed.	Sep 22,2010 03:19:12 PM	10.52.194.164
Major	IF-10.52.110.193	Interface failure. Status poll failed.	Sep 22,2010 03:18:43 PM	10.52.194.164
Major	IF-10.52.110.225	Interface failure. Status poll failed.	Sep 22,2010 03:18:02 PM	10.52.194.164
Major	IF-10.52.110.241	Interface failure. Status poll failed.	Sep 22,2010 03:17:41 PM	10.52.194.164
Warning	10.52.194.164;xemRemoved-1	XEM removed - sysUpTime: 0 hours, 5 minutes, 51 seconds., snm...	Sep 22,2010 03:14:29 PM	10.52.194.164

FIGURE 27-19 Alarm View Main Panel

27.8 Alarm Propagation

In a network, components (managed objects) are in a hierarchy, and faults at one level usually affect the status of another level. Network administrators need to understand how the AlliedView NMS reports and propagates alarms so that they can control what alarms appear in the Alarm View and quickly locate and resolve them.

Refer to Figure 27-20 while reading this section, since it helps show the types of methods used to obtain the status of an object and the objects relationship to the network hierarchy.

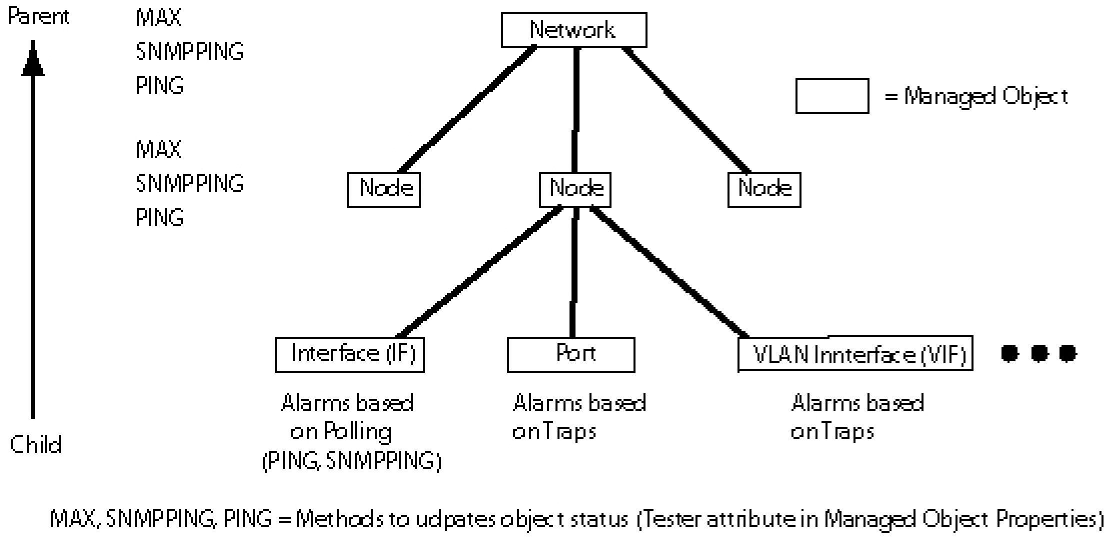


FIGURE 27-20 Alarm Propagation Hierarchy

There are various methods used to get the status of a managed object:

- PING - This uses ICMP for polling, and so uses a simple traceroute to see of the object responds. If there is no response, an alarm (usually MAJOR) is produced.
- SNMPPING - This uses an SNMP GET for polling, and waits for a response. If there is no response, an alarm (usually MAJOR) is produced. Moreover, if there is no response within 5 seconds, there is an additional time out alarm.
- Traps - These are the unsolicited messages that are sent by the device, with a resulting alarm.
- MAX - This is not an actual method (there is no direct communication with the object), but a rolling up of the status results of an object and its children objects and a reporting of the alarm of the highest severity. The examples below will explain this in greater detail and show how this works.

The main concepts for alarm propagation up the hierarchy are as follows:

- The status of an object is the highest severity alarm for that object.
- When alarms are propagated, the highest alarm of all children is what gets propagated (if parent set to MAX).
- The severity of an alarm on the parent object (node) is the highest severity for that node, including the severities that are propagated (if parent set to MAX).

27.8.1 Controlling Alarm Propagation

While referring to Figure 27-20, consider the following examples:

27.8.1.1 Example 1 - Parent Object set to Max for Polling-Based Alarms (default)

- The administrator sets the Tester attribute for interfaces (IF) in the MO Property Form to PING or SNMPPING, so if an interface fails, a major alarm is reported by the interface.

- For the parent node, the administrator sets the Tester attribute to Max.

The result of this set up is as follows:

- If an interface fails, the alarm is reported at the node level, with the text of the alarm "one or more interfaces have failed."
- Since an alarm at the interface level will result in an alarm at the node level, the node level alarm is not cleared until all interface alarms have been set to CLEAR by the AlliedView NMS.
- If the parent node has a failure of higher severity, the parent node will take precedence.

Note that this concept of propagating alarms up the hierarchy works at both the Node and Network level; the node reports among the interfaces the highest level of alarm, while at the network level, MAX means the network reports among the nodes the highest level of alarm. Alarms at the node level would be propagated to the network object with the text "One or more Nodes have a Major Alarm."

27.8.1.2 Example 2 - Parent Object set to PING/SNMPPING (not Max) for Polling-Based Alarms

In this scenario, the higher level object is not set to Max, but to PING/SNMPPING. The following occurs:

- The higher level object will only poll the primary IP interface of its child object.
- There is less "sensitivity" of the higher level object to lower level alarms, since other alarms at the lower level are not reported to the higher object.

27.8.1.3 Example 3 - Parent Object set to Max for Trap-Based Alarms

Note: The function of the MAX value for objects that use traps to produce alarms is the same of those produced by traps. This is made a separate example to highlight certain differences.

- For a port, the administrator does **not** use the Tester attribute, since alarms are reported by the unsolicited trap.
- For the parent node, the administrator sets the Tester attribute to Max.

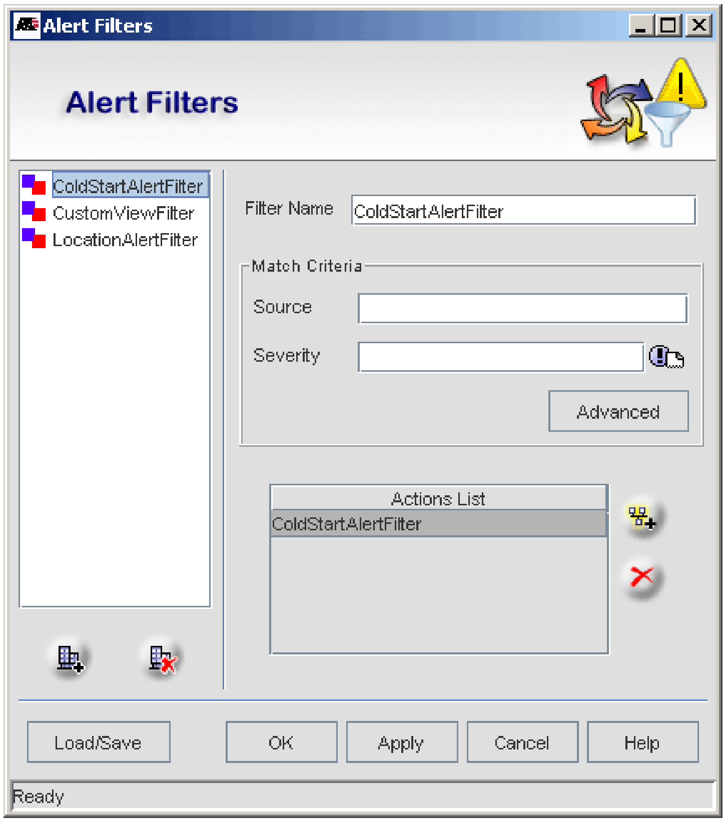
The result of this set up is as follows:

- If a port has a trap, the alarm is reported at the node level.
- When a port has recovered and a Link UP trap is received by the AlliedView NMS, this is still a trap and therefore the CLEAR status "alarm" would be reported to the parent level.
- When a port has recovered on the device and a Link UP trap is not received by the AlliedView NMS, the node would still show an alarm.
- If the parent node has a failure, the parent node will take precedence.

27.9 Configuring Alarm Filters

Alert filters are used to filter and modify the properties of an incoming alert. When the alert matches specified criteria, an action (such as sending an email) will occur.

To parse alarms, select *Edit -> Configure -> Alarm Filters* from the main menu of the Alarms Panel. The **Alert Filter Configuration** form appears as shown in Figure 27-21.



ColdStartAlertFilter
CustomViewFilter
LocationAlertFilter

Filter Name: ColdStartAlertFilter

Source:

Severity:

Actions List
ColdStartAlertFilter

Ready

FIGURE 27-21 Alert Filter Configuration Form

This form allows the Administrator to configure both the alert filter (the left side of the screen) and the filter action (the right side of the screen).

Note: Many of the actions and fields are similar to setting Event Filters, so there are references when appropriate

The user can add, modify, or delete an Alert Filter from the left side of the form. Refer to Table 27-5 for a summary of match criteria.

At least one action needs to be associated with the incoming filtered alarm. For an alarm filter, click under filter action to add one of the action types. These types are explained in Event Filter Actions.

27.9.1 Example to Configure Alarm Filter and Actions

27.9.1.1 Summary Procedure

Adding an alarm filter and an action is done as follows.

Note: An alarm filter must have at least one action.

1. Click in the Alert Filter panel.
2. Modify the alert filter name as needed and the match (Source and Severity) criteria fields. If needed, expressions can be used: wildcard (*), negation (!), and separators (,). Use the More option if needed.
3. Click in the Alert Filter Action panel to activate the Action Type panel.
4. Click one of the buttons for each action type and select **New** or **Edit**.
5. Fill in the Action Details panel, and then click **Update Action**. The **Update Action** button changes to **Update Filter**.
6. To add more actions, click **Add** in the Alert Action panel and add more action types and details.
7. Cancel any filters or actions by clicking **Cancel** as they appear in context.
8. If desired, reorder the resulting alert filters and actions by dragging and dropping.

To modify an alert filter, select a filter from the list and make any changes, and then click **Apply** to make the changes permanent.

To delete an alert filter, select a filter and click the **Delete icon** from the Alert Filter panel. Any associated action will also be deleted. To delete a filter action, select an action from the Configured Filter List, and then click the **Delete** icon from the Alert Filter action panel.

To load a set of alert filters from a file, click **Load**/Save. A dialog box prompts for the file path to read the filters from. Click **Load** to load the filters.

To save a set of alert filters (for later use or as a backup), click **Save**. A dialog box prompts for the file path to write the filters to. Click **Save** to save the filters.

When saving these files, the AlliedView NMS sets as the default directory the `<NMS Home>/state` directory, so for example the file path:

../conf/alert.filters

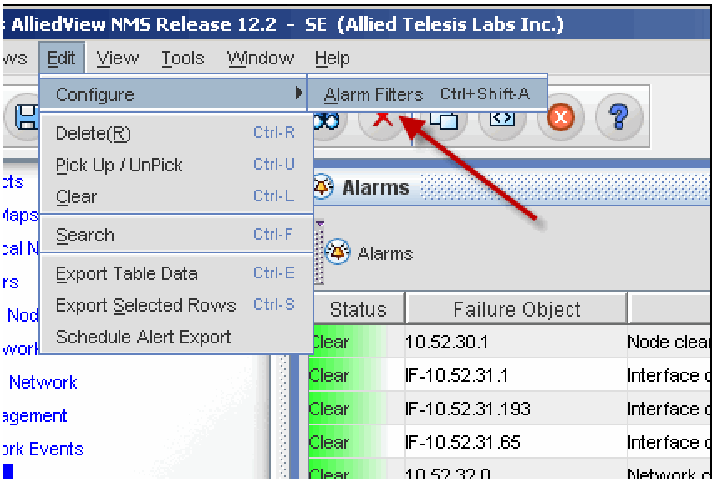
is being saved in the `conf` directory by going up one level from the `state` directory (..) and then down to the `conf` directory. If the user enters in the form only a file name, that file is being saved in the default `state` directory.

If any changes are made and the window is closed without clicking **Apply**, a prompt will appear asking whether to make the changes.

27.9.1.2 Detailed Procedure

A step-by-step procedure procedure shows how to take alarms from iMGs with an IP address fo 10.10.50.*, and eliminate alarms that comes in with the text “Unable to login to this device..” .

1. Select *Edit –> Configure -> Alarm Filters* to access the Alert Filters window, as shown in Figure 27-22.

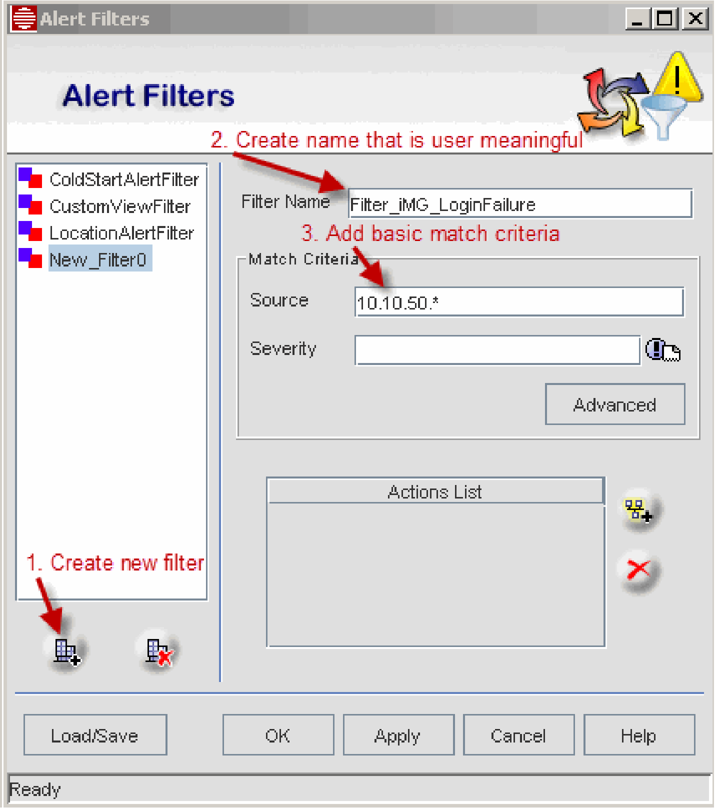


Status	Failure Object	
Clear	10.52.30.1	Node clea
Clear	IF-10.52.31.1	Interface c
Clear	IF-10.52.31.193	Interface c
Clear	IF-10.52.31.65	Interface c
Clear	10.52.32.0	Network c

FIGURE 27-22 Accessing the Alert Filters Window

2. Create the filter and set up the basic criteria for filtering. The steps would be:

   1. Select the button on the bottom left.
   2. Rename the filter to something that will indicate its use.
   3. Add a match criteria. Here the source is the incoming address and it can be wild-carded by using the "*".
   4. Refer to the following figure, which displays these three steps.



2. Create name that is user meaningful

Filter Name: Filter_iMG_LoginFailure

3. Add basic match criteria

Source: 10.10.50.*

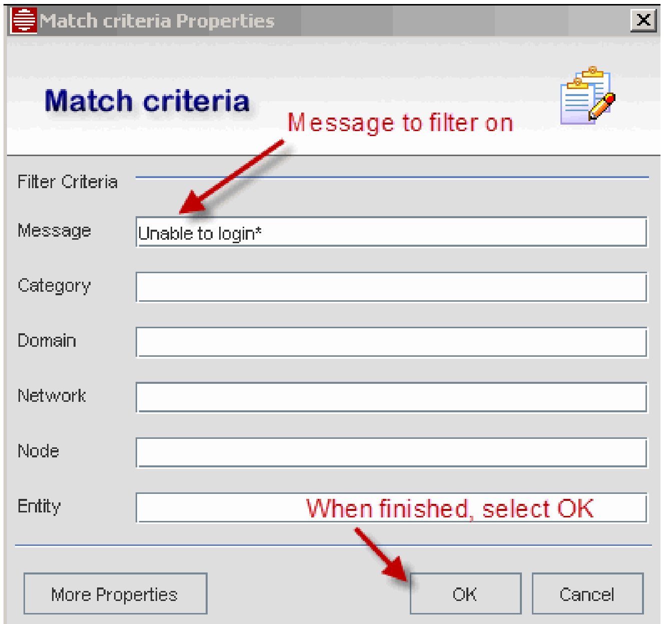
Severity:

1. Create new filter

Ready

FIGURE 27-23 Create Alert Filter with Basic Match Criteria

3. To create a criteria beyond the Source and Severity, select **Advanced**. The *Match Criteria Properites* sceen appears.
4. In this example we will setup a filter to eliminate an alarm that comes in with the message “Unable to login to this device….”. Enter this using a wildcard in the Message field as shown in Figure 27-24, then select **OK**.



Match criteria Properties

Match criteria

Message to filter on

Message: Unable to login*

When finished, select OK

FIGURE 27-24 Setting Advanced Filter Criteria

5. Back on the *Alert Filters* screen, we need to associate it with some action to take. We create the filter action by clicking on the add button (next to the Actions List). This brings up the *Add action* screen, as shown in Figure 27-25.

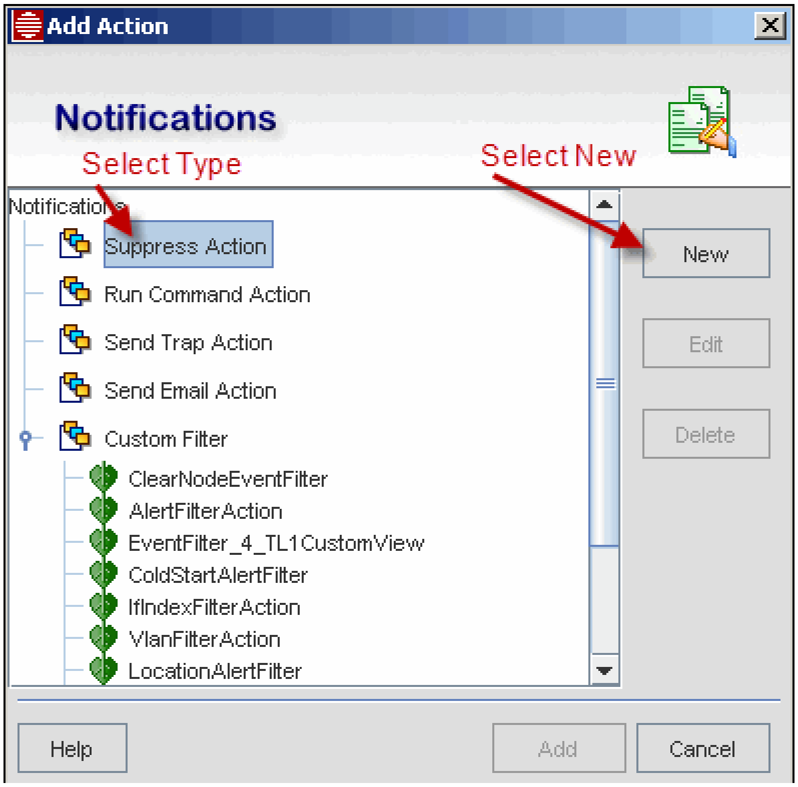
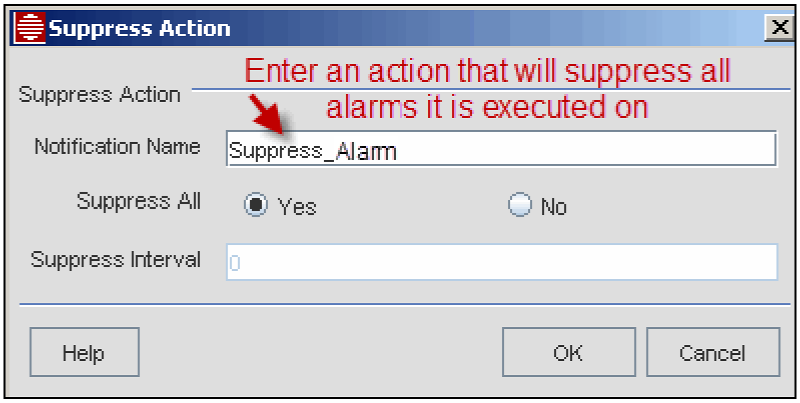


FIGURE 27-25 Add Action Window (Notifications when Criteria Met)

6. Since we want to suppress the "Unable to Login.." alarm so that we no longer see it in the alarm list, select the **Suppress Action** type and **New**.button, as shown in Figure 27-25. The Suppress Action window appears, as shown in the Figure 27-26.


Suppress Action
Enter an action that will suppress all alarms it is executed on
Help
OK
Cancel

Suppress Action

Notification Name: Suppress_Alarm

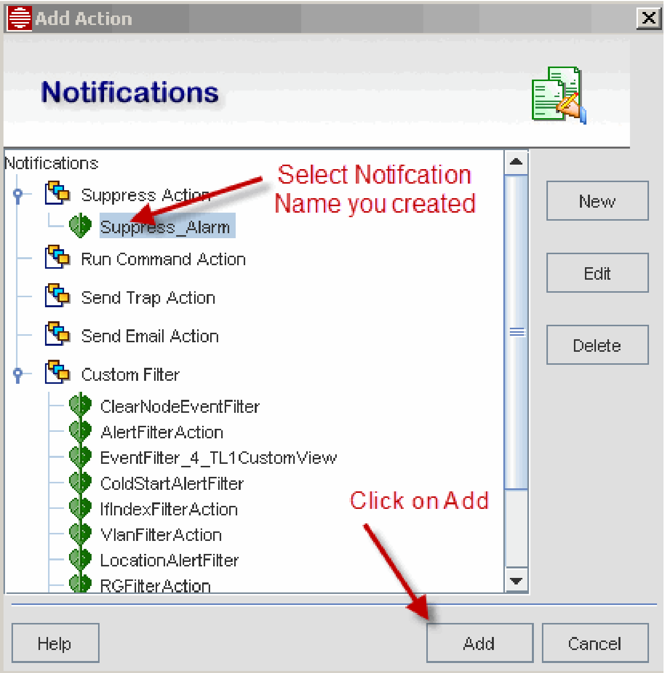
Suppress All: ● Yes ○ No

Suppress Interval: 0

FIGURE 27-26 Enter Notification Name

7. Add the Notification Name (in this case Suppress_Alarm), and Click **OK,** as also shown in Figure 27-26.

8. Back on the *Add Action* screen, select the Noticfication Type you created (here **Suppress_Alarm**) and Select **Add**, as shown in Figure 27-27.

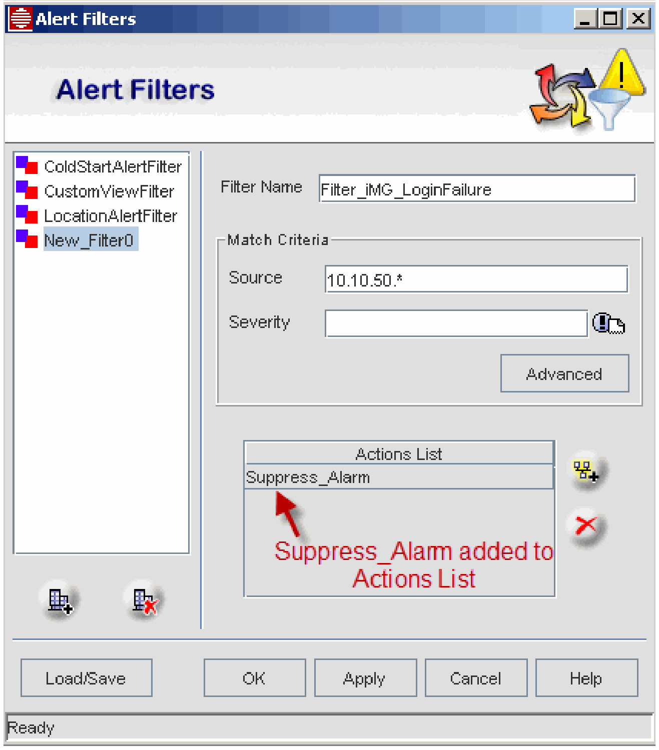


Select Notifcation Name you created

Click on Add

FIGURE 27-27 Adding an Action to the Alert Filter

9. This returns you to the *Alert Filters* window, and Suppress_Alarm is added to the Actions List. Refer to Figure 27-28.



Filter Name Filter_iMG_LoginFailure

Source 10.10.50.*

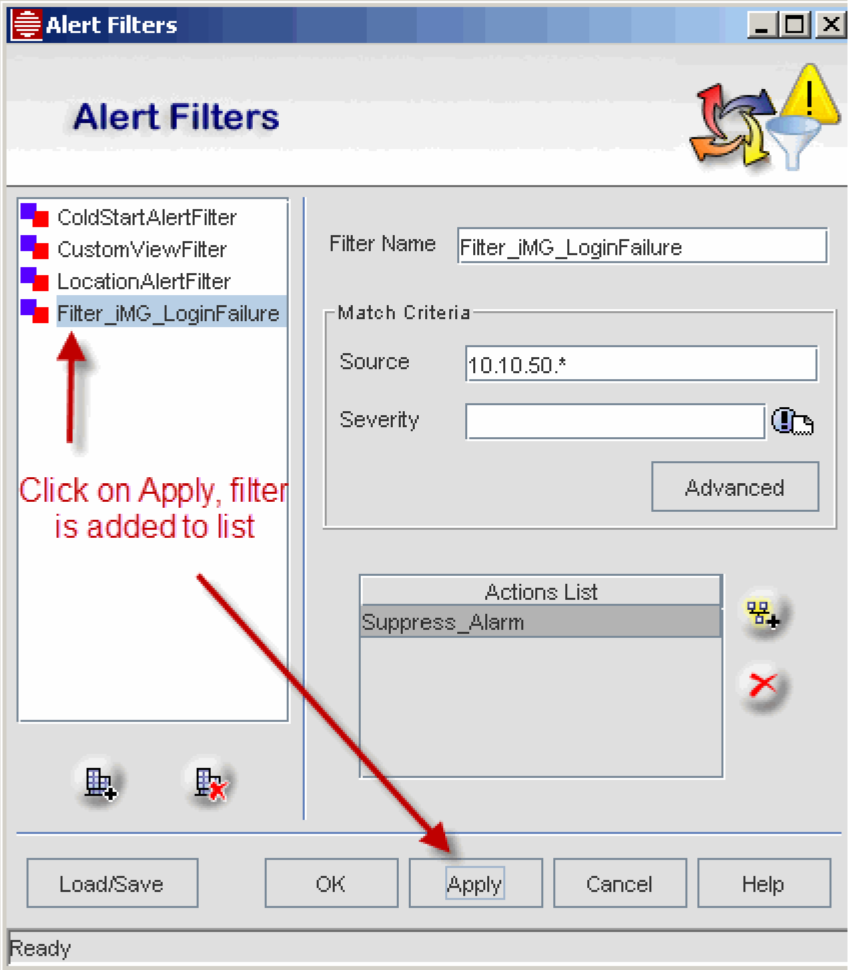
Severity

Actions List
Suppress_Alarm

Suppress_Alarm added to Actions List

FIGURE 27-28 Actions List Complete

10. With the attributes for the Alert Filter complete, click on **Apply**. The new filter name (Filter_iMG_LoginFailure) is now added to the list of Alert Filters, and this filter will be applied when processing alarms. Refer to the following figure.



Filter Name: Filter_iMG_LoginFailure

Match Criteria

Source: 10.10.50.*

Severity:

Actions List: Suppress_Alarm

FIGURE 27-29 Alert Filter added to List

11. With the Alert Filter added, Click on Load/Save. This brings up the Filter Details window that allows you to save the filters to the `alert.filters` file. Click on **Save**. The file can then be loaded for later use.

12. With the procedure complete, click on **OK**. The *Alert Filters* window closes.

27.10 Alarm Retrieval for iMAP Devices During Rediscovery

When you rediscover iMAP devices, you can choose to retrieve previous alarms. When you select this option the following occurs:

- Alarms are retrieved using the CLI.
- The alarms are parsed and converted to events.
- The events are processed by Alarm Management and can be parsed, filtered, customized, and have other actions associated with them.
- After processing, the events are added to the the NMS database so that they can be included in the Events and Alarms displays.

If an alarm that previously existed no longer exists after the device is rediscovered, the NMS shows the alarm as cleared.

All retrieved alarms include the text “Retrieved:true” in the message of the event or alert to indicate that they were retrieved during rediscovery.

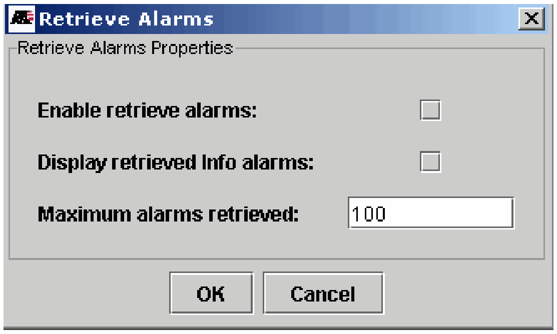
27.10.1 Enabling and Disabling Alarm Retrieval

You must have administrator (or root) permissions on the NMS server.

To enable or disable alarm retrieval:

1. Navigate to the `<NMS_Home>/bin/` directory, where `<NMS_Home>` is the directory where the NMS is installed.
2. Double-click or run the following file from a command line:
   - AT_RetrieveAlarmsSetup.bat (Windows)
   - AT_RetrieveAlarmsSetup.sh (Linux)

   The **Retrieve Alarms** box appears:



Retrieve Alarms Properties

Enable retrieve alarms: □

Display retrieved Info alarms: □

Maximum alarms retrieved: 100

FIGURE 27-30 Retrieve Alarms

Option	Description
Enable retrieve alarms	Enables alarm retrieval on iMAP devices.
Display retrieved Info alarms	Displays retrieved alarms with a severity of “Info”.
Maximum alarms retrieved	Number of retrieved alarms per device to process and display. If this number is lower than the number of retrieved alarms the lowest severity alarms will be ignored.

3. Select the desired options, then click **OK**.

27.10.2 Interactions with Traps

The NMS alarm management system uses traps as a source for device alerts. The following interactions exist between alarm retrieval and retrieval of device changes through traps:

- Some retrieved alarms do not have enough information to be correlated to the corresponding alarms that were received through traps.
- Some retrieved alarms do not have the corresponding alarms received through traps, and some of the alarms received through traps do not have the corresponding alarms that can be retrieved from the device.
- Default severities used when displaying retrieved alarms are specified in the device. Alarms received through traps have default severities defined in the NMS.

27.11 Forwarding SNMP Traps

You can forward SNMP traps to one or more IP addresses for SNMP monitoring. The NMS uses configuration files to control trap forwarding. Configuring the NMS to forward SNMP traps involves four main tasks:

1. Copy and rename the required configuration files.
2. Customize the forwarding file.
3. Modify the filtering file.
4. Restart the NMS server.

27.11.1 Renaming Configuration Files

1. Navigate to the `<NMS_Home>/conf/` directory, where `<NMS_Home>` is the directory where the NMS is installed.
2. Copy and paste the following files in the directory:

```
AT_Trap.forward
trap.filters
```

3. Rename the copies as follows:

File	New Filename
Copy of AT_Trap.forward	trap.forwarder
Copy of trap.filters	trap.filtersOriginal

When you are done the following four files should be present in the directory:

- AT_Trap.forward
- trap.forwarder
- trap.filters
- trap.filtersOriginal

27.11.2 Customize the Forwarding File

1. Open the file `trap.forwarder` in a text editor.
2. Scroll down to the bottom of the file. You should see the following lines of text:

```
-->

<TRAP-FILE
  Refresh_Time="10"/>
```

```
<TRAP-REDIRECTION
Dest_Addr="192.168.4.50"
Dest_Port="162"/>

</TRAP-FORWARDER>
```

3. Modify the **Dest_Addr** and **Dest_Port** lines to include the destination IP address and port for your implementation.
4. To forward traps to multiple destinations, add and modify additional **<TRAP-REDIRECTION** sections:

```
<TRAP-REDIRECTION
Dest_Addr="192.168.1.49"
Dest_Port="162"/>

<TRAP-REDIRECTION
Dest_Addr="192.168.1.179"
Dest_Port="162"/>
```

5. If necessary, modify **Refresh_Time="10"** to a different interval value. This is the interval, in seconds, that the NMS checks the file for updates.

Note: *If you set Refresh_Time="0", the NMS will only read the file when you start the NMS server. For the NMS to capture changes while the NMS is running, the refresh time must be 1 or greater.*

6. Save and close the file.

27.11.3 Modify the Filtering File

1. Open the file `trap.filters` in a text editor.
2. Search on the term **RedirectionTrapFilter**. This should take you to the following section:

```
<!--  trap forwading filter - uncomment to enable
      this will forward all v1/v2 traps to target agent
      specified in conf/trap.forwarder

 <FILTER
  name="RedirectionTrapFilter"
  classname="com.telesyn.nms.fault.server.traps.RedirectionTrapFilter"
  enable="true"
  GT="*"
  ST="*"
  enterprise="*"/>
 <FILTER
  name="RedirectionTrapFilterv2c"
  classname="com.telesyn.nms.fault.server.traps.RedirectionTrapFilter"
  enable="true"
  trapoid="*"/>
-->
```

3. The **<!--** and **-->** at the beginning and end of the section, respectively, indicate the section is commented out and the commands on it will not be executed. To enable SNMP trap forwarding, you need to uncomment the part of the section with active commands, beginning with the first **<FILTER** statement. To uncomment the pertinent section, move the bottom **-->** to above the first **<FILTER** line. The revised section should look like this:

```
<!--  trap forwading filter - uncomment to enable
      this will forward all v1/v2 traps to target agent
      specified in conf/trap.forwarder

-->


 <FILTER
  name="RedirectionTrapFilter"
  classname="com.telesyn.nms.fault.server.traps.RedirectionTrapFilter"
```

```
        enable="true"
        GT="*"
        ST="*"
        enterprise="*"/>
       <FILTER
        name="RedirectionTrapFilterv2c"
        classname="com.telesyn.nms.fault.server.traps.RedirectionTrapFilter"
        enable="true"
        trapoid="*"/>
```

4. Save and close the file.

27.11.4 Restart the NMS Server

You must restart the server to have the NMS recognize the renamed `trap.forwarder` file. Once the NMS recognizes the file, you can make further changes to it without having to restart the server. The NMS checks for updates in the file based on the **Refresh_Time** interval you set.

28. Built-in Browsers - SNMP MIB and CWMP

28.1 SNMP MIB

Management Information Bases (MIBs) are a collection of definitions that define the properties of the managed objects. To enable a management application to operate intelligently on the data available on the managed device, the manager needs to know the names and types of managed objects in the device. This is made available by the MIB modules. A MIB describes a set of managed objects.

Each property of a managed object in a MIB has a unique identifier. This identifier consists of the type of the object (such as counter, string, gauge, or address), the access level (such as read or read/write), size restrictions, and range information. It should be understood that a MIB is only an abstraction of data available on the managed device and not a physical database or a physically executable object.

Use the following table to locate the task you wish to perform. If you are using the NMS, use the Screen Name as well to locate the relevant section.

TABLE 28-1 Task List for MIB Manager

Task	Screen / Form Name (if Applicable)	Section
Review Screen Areas		"MIB Browser Screen and Toolbar" on page 1037
Load / Unload MIBs	Object Properties	Overview "Overview" on page 1038 Loading Options "Loading Options (Directly, as Compiled Files, Using MySQL)" on page 1039 Loading as Compiled Files "Loading MIBS as Compiled Files" on page 1039 Loading from Database "Loading MIBs from a Database" on page 1040 Loading with MySQL[1] "Loading MIBs Using MySQL" on page 1040 Unloading "Unloading MIBs" on page 1041
Set MIB Browser Settings	MibBrowser Settings	"MIB Browser Settings" on page 1041
Perform GET, GET NEXT, GET BULK, SET		"SNMP Operations" on page 1041
View SNMP Table Data		"MIB Browser – Table Operations" on page 1042
View Traps		"Trap Viewer" on page 1044

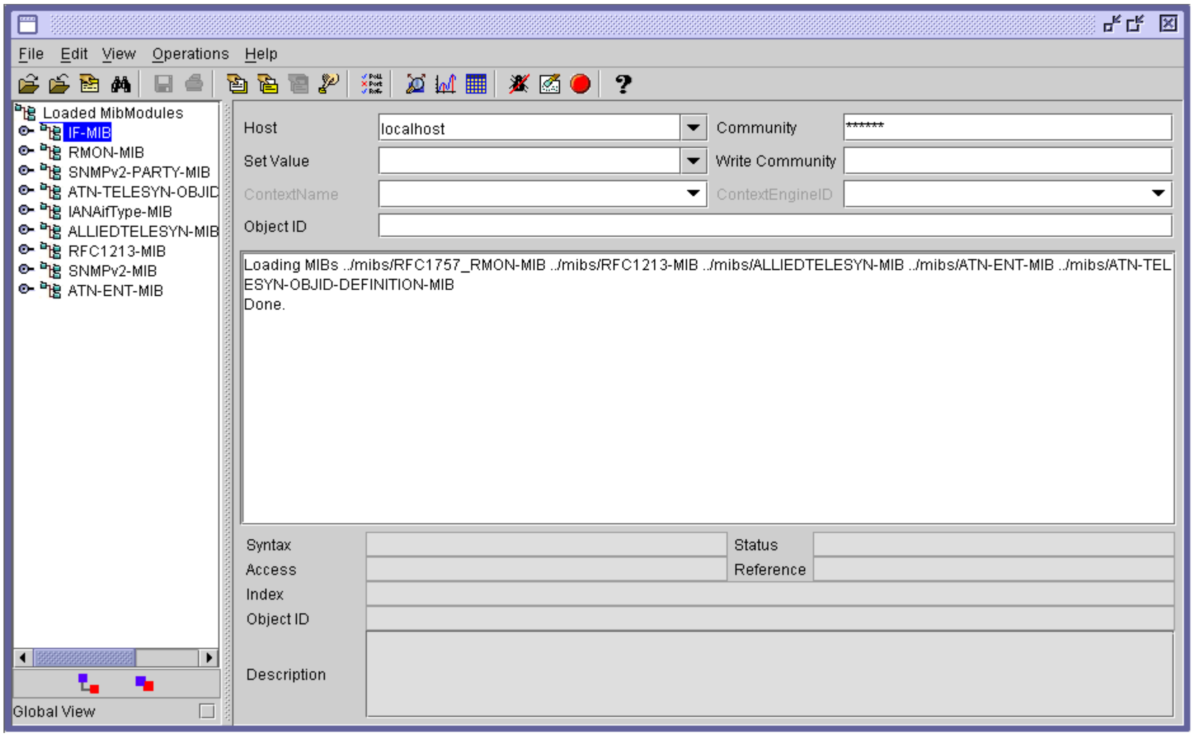
TABLE 28-1 Task List for MIB Manager (Continued)

Task	Screen / Form Name (if Applicable)	Section
Create Trap Parser File		Overview "Trap Parser" on page 1045 Create Parser File "Procedure to Create a Parser File" on page 1047 Add Trap Definitions "Adding a Trap Definition from MIBs to a Parser File:" on page 1048 Filter Incoming Traps "Filtering Incoming Traps" on page 1048 Setting Parser Parameters "Setting Trap Parser Parameters" on page 1048
Plot SNMP data		"Graphs" on page 1049

1. Registered Trademark ® 2003 MySQL AB. All rights reserved.

28.2 MIB Browser Screen and Toolbar

The information contained in the MIBs can be retrieved and viewed by accessing the MIB Browser from the Tools menu. The Mib Browser panel is shown in the following figure.



Host: localhost

Community: ******

Set Value:

Write Community:

ContextName:

ContextEngineID:

Object ID:

```
Loading MIBs ../mibs/RFC1757_RMON-MIB ../mibs/RFC1213-MIB ../mibs/ALLIEDTELESYN-MIB ../mibs/ATN-ENT-MIB ../mibs/ATN-TEL
ESYN-OBJID-DEFINITION-MIB
Done.
```

FIGURE 28-1 MIB Manager View

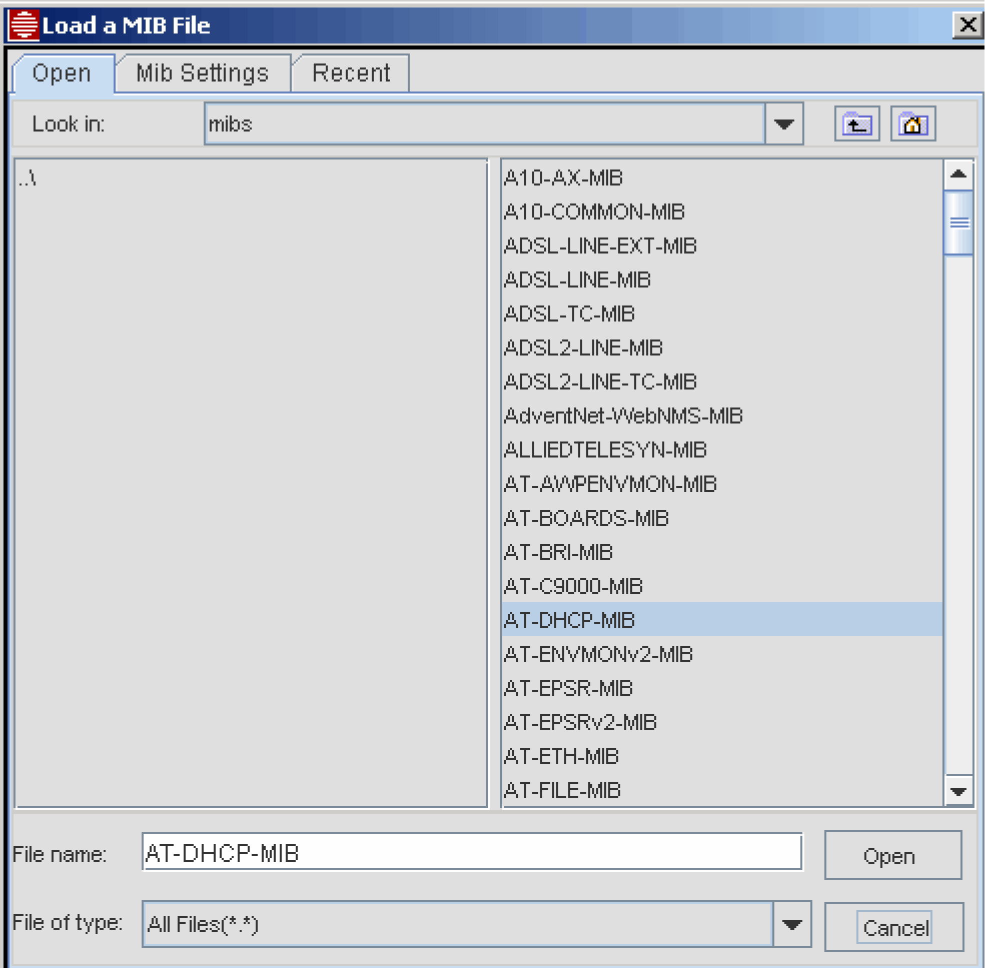
The operations allowed with the Mib Browser are available through the series of icons in the Toolbar at the top of the Mib Browser's main window. You can hide the Toolbar by de-selecting the ToolBar item in the view menu. The Menu Bar is also available for doing all operations.

28.3 Loading and Unloading MIBs

28.3.1 Overview

To load the MIB files in the Mib Browser, use the **LOAD MIBs** button or select *File -> Load MIB* menu item. This brings up the **Load a Mib File** Screen as shown in the following figure.

Note: The MIB Browser for NMS is strict on syntax, and if there is an error, such as an extra comma in the object type list, the MIB will not load.



Look in: mibs

..\

A10-AX-MIB
A10-COMMON-MIB
ADSL-LINE-EXT-MIB
ADSL-LINE-MIB
ADSL-TC-MIB
ADSL2-LINE-MIB
ADSL2-LINE-TC-MIB
AdventNet-WebNMS-MIB
ALLIEDTELESYN-MIB
AT-AWPENVMON-MIB
AT-BOARDS-MIB
AT-BRI-MIB
AT-C9000-MIB
AT-DHCP-MIB
AT-ENVMONv2-MIB
AT-EPSR-MIB
AT-EPSRv2-MIB
AT-ETH-MIB
AT-FILE-MIB

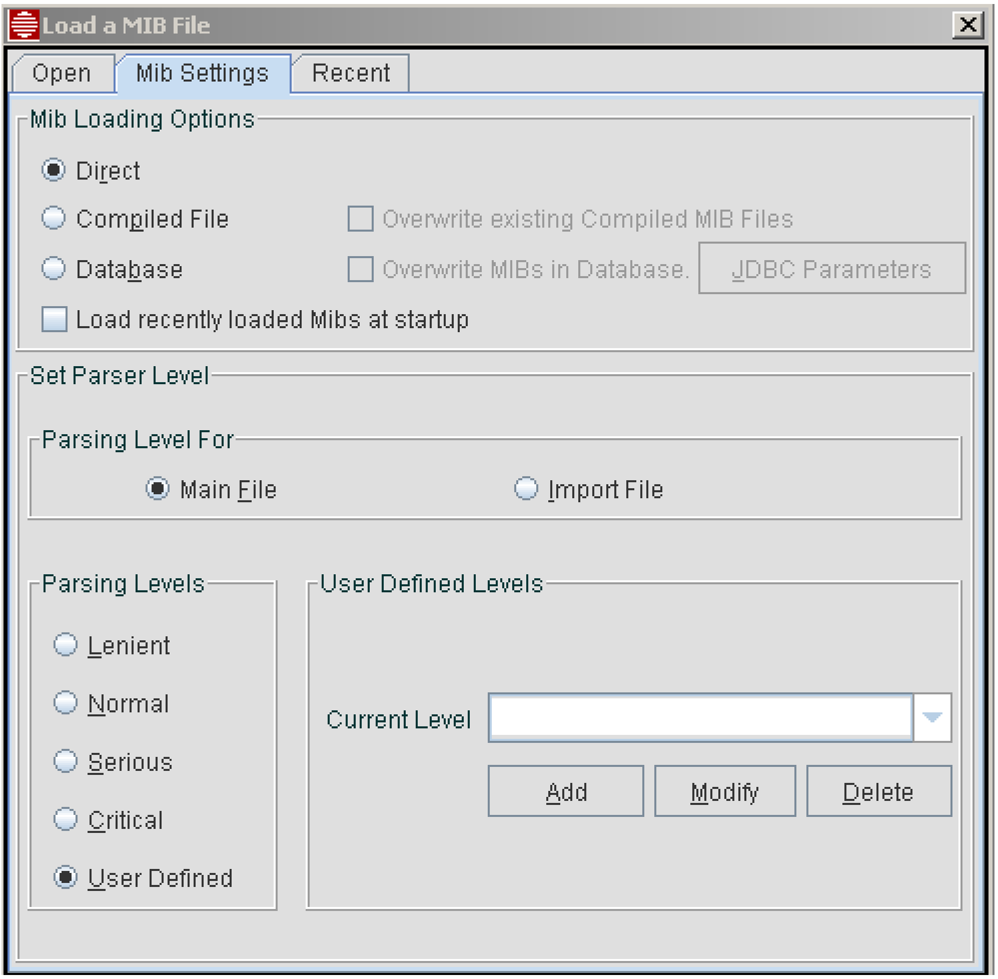
File name: AT-DHCP-MIB

File of type: All Files(*.*)

FIGURE 28-2 Load MIB File Screen

28.3.2 Loading Options (Directly, as Compiled Files, Using MySQL)

The Mib Browser has the following Mib Settings for loading the MIBs, as shown in the following figure.



Mib Loading Options

● Direct

○ Compiled File □ Overwrite existing Compiled MIB Files

○ Database □ Overwrite MIBs in Database.

□ Load recently loaded Mibs at startup

Set Parser Level

Parsing Level For

● Main File ○ Import File

Parsing Levels

○ Lenient

○ Normal

○ Serious

○ Critical

● User Defined

User Defined Levels

Current Level

FIGURE 28-3 Options for Loading MIBs

- Loading MIBs directly.
- Loading MIBs as compiled files.
- Loading MIBs from database.

You can also load MIBs directly in plain text format, although for large MIBs the loading time will be higher.

The **Recent** tab lists all the recently loaded MIBs. The MIBs that are listed can be opened by selecting the tic box and then the Open button.

28.3.3 Loading MIBS as Compiled Files

The Mib Browser allows loading of compiled MIB files. The compiled MIB files reduce loading time, leading to performance improvement. To store the compiled file information, there are two file types used for storing the MIB information in a formatted structure:

- **.cmi** - This file type contains MIB information like MibNode, MibModule, naming hierarchy, etc.
- **.cds** - This file type contains the description and reference of the nodes in the Mib.

The compiled MIB files reduce the loading time, leading to performance improvement. The applications and the applets have the option of loading the MIB files directly or as compiled MIB files. The **Load MIBs from compiled File** option is provided in the dialog box to decide whether to load MIB from compiled MIBs or not. By default, this option is enabled. If this is unchecked, the user can directly load the MIB file as provided.

When **Load MIBs from compiled File** is selected, the Mib Browser tries to load the **.cmi** and **.cds** files, if they are present. Otherwise, this parses the MIB file and writes the output in **.cmi** and **.cds** files, and then loads the MIB file. For example, for the RFC1213-MIB the compiled MIB files are *RFC1213-MIB.cmi* and *RFC1213-MIB.cds*. The advantage of using this option is that the MIB need not be parsed each time it is loaded, which reduces the load time.

To load the compiled MIBs, load the **.cmi** file alone. The **.cmi** file will have reference to the **.cds** files. The **mib_file_name.cds** file should not be loaded directly.

28.3.4 Loading MIBs from a Database

The Mib Browser allows loading MIB files from the database. The MIB files can be stored in any RDBMS such as MySql or Oracle[1]. Applications can load these MIB files directly from the database. This feature is particularly useful for a high number of MIB files.

The Mib Browser uses JDBC (Java Database Connectivity) for the database support. Applications should use a valid class 3 JDBC driver of the respective databases to enable the database support.

To add database support for loading the MIBs, applications should initialize the necessary database parameters first. The following details have to be given in the settings dialog:

- DriverName - Name of the DataBase driver.
- URL - URL pointing to the DataBase filename.
- userName - userName.
- passWord - password.

When the **Load MIBs From Database** is enabled in the load options dialog box, the Mib Browser tries to load the MIB file from the database. If the MIB files are already present in the database, the result will be successful. If the MIB files are not present in the database but are available only in the local path in which the application is executed, the MIB files are loaded in the database for the first time, and then loaded in the application.

A few MIB modules are provided in the MIBS directory, i.e. RFC1213-MIB, RFC1271-RMON, RFC1155-SMI, RMON2-MIB, TOKEN-RING-RMON-MIB and RFC1315-FRAME. It may be convenient to copy your MIB module files to be loaded into the mibs directory.

28.3.5 Loading MIBs Using MySQL

The following database parameters have to be configured in the application:

- driver name - org.gjt.mm.mysql.Driver
- url - JDBC: mysql://< machine name > / < database name >
- username - < a valid user name >
- password - < password for the above user >

The jar file **mysql_comp.jar** has to be included in the classpath. If the jar is not in the classpath, the following exception is thrown:

Input: Java.lang.ClassNotFoundException:org.gjt.mm.mysql.Driver

For other databases, please use the equivalent parameters.

[1] Registered Trademark ® 2003 Oracle Corporation. All rights reserved.

28.3.6 Unloading MIBs

To unload the loaded MIB, select the node of the MIB Tree then click the **UNLOAD MIB** icon or select the *File -> UnLoad MIB* menu item. This removes the MIB Tree of the unloaded MIB

28.4 MIB Browser Settings

The Mib Browser can be used for MIB browsing and to view and operate on available data through an SNMP agent. The Mib Browser allows configuration of various options needed for SNMP operations.

To set the various options, click the **SETTINGS** icon, or select the *Edit -> Settings* menu item. This brings up a dialog box where the following options and their default values are set. The user can modify the default values as needed, as shown in the following table.

TABLE 28-2 MIB Browser Settings

Options	Default Values	Other Values
Snmp Version	V1	V2c or V3
Snmp Port	161	Any user- defined port
Time out	5 sec	Any user-defined value
Max repetitions	50	Any user-defined value
Graph Type	Line Graph	Bar Chart
Trap Port	162	Any user-defined port
Retries	0	Any user-defined value
Non-repeaters	0	Any user-defined value

FIGURE 28-4 MIB Browser Settings

28.5 SNMP Operations

The Mib Browser allows the user to do the typical SNMP operations, such as GET, GET NEXT, GET BULK and SET.

To perform the GET operation, the user has to load the MIB file, select the desired node, and click the **GET** icon or choose the *Operations -> Get* option from the menu bar. To fully specify an object to an SNMP agent, both the Object ID (which defines the type of object), and the instance (the specific object of the given type) need to be provided. From the MIB, the Object ID can be obtained to which an instance needs to be added to completely identify the object of interest. For non-tabular (or scalar) objects, this is simply an instance of 0 (for example, sysDescr.0). This need not be specified; the Mib Browser adds it to the selected node. For tabular objects, the instance is defined by the MIB and is a sequence of one or more variables (for example, ifInOctets.2 or tcpConnState.179.74.15.126.1192.225.226.126.197.80).

You also need to specify the hostname and community string of the SNMP agent you are talking to in the appropriate field.

To talk to a V3 agent, choose the Version3 from the choice box in the **Settings** dialog and also make sure that the v3 parameters are set in V3 Settings Dialog.

28.5.1 Multi-Varbind Request

Select the *Display -> Multi-Varbind* menu item from the *View* menu to view the Multi-Varbind panel. To do a multiple varbind request, select the leaf node and append the instance, and then click **Add**. This adds the OID given in the Object Identifier field and the Value given in the SetValue field both separated with a colon to the list. If a value is not given in the SetValue field, the NULL value is appended. We can add multiple numbers of OIDs and values like this. Ensure that you check the

Multi-var checkbox before doing a SNMP operation for multiple varbind SNMP request. Otherwise, it will do a request for the OID in the Object Identifier field.

To do multiple-variable SNMP SET, ensure that the proper OIDs and values are given in the text fields before adding them to the list. Check the **Multi-Var** check box before doing the multiple variable SET.

To delete the varbind(s) from the list select the varbind(s) from the list and click **Delete** to delete the varbind(s) from the list.

To edit the varbinds added in the list, select a varbind and click **Edit**. This shows an OID and the Value of the varbind in the TextFields to edit the OID and the Value. Edit it and press **OK** button to modify the OID and the value or click **Cancel** to restore the old values.

- To perform a GET operation, click the GET icon () or select the *Operations -> Get* menu item. If the MIB node and instance are specified, this gets all objects under the selected MIB object or the specific object.
- To perform a GETNEXT operation, click the GETNEXT icon () or select the *Operations -> GetNext* menu item. If a MIB node is specified, this gets the next object after the specified object or the specific object instance.
- To perform a GETBULK operation, click the GETBULKicon () or select the *Operations -> GetBulk* menu item. This gets a sequence of Next Objects immediately after the specified object. The number of Object instances returned is equal to the Max-Repetitions field v2 & v3.

Note: Max Repetitions cannot exceed 200.

- To perform a SET operation, click the SET icon () or select the *Operations -> Set* menu item. This enables setting the value of the specified object, based on the value in the Set Value field. To do a SET for Octet String Type in hex format, enter the bytes in hex format with each bytes separated by a colon and the entire string within single quotes. For example, to give 0xff0a3212 enter 'ff:0a:32:12' in the SetValue field.

28.6 MIB Browser – Table Operations

The Mib Browser provides a user-friendly way for viewing SNMP Table data. The table data can be viewed in a separate window called SNMP Table Panel. The SNMP Table Panel provides various options for table handling, such as adding a row to the existing table, viewing graphs, index editor, etc.

Perform the following steps to view the SNMP table in the SNMP Table Panel:

1. Make sure the appropriate MIBs have been loaded.
2. Specify the proper agent hostname or IP address in the host field of the MibBrowser.
3. Specify a valid OID - the OID needs to be a Table OID.
4. The OID can be chosen by browsing the MIB in the MIB Tree.

To view the SNMP Table, click the **SNMP TABLE** icon or select the *View -> SNMP Table* menu item. If the selected OID is a table, this displays an SNMP table. In the SNMP table, click **Start** to get the columnar objects.

The following table explains the options available

TABLE 28-3 **SNMP Properties**

Option	Functions for SNMP Properties
Page	It has two options - origin and index. If the option origin is enabled, the table retrieval is done from the origin. If the index is enabled, the user can set an index value in the adjacent text field from which the table is retrieved.
Host	The value set here overrides the host name set in the Mib Browser settings dialog box.

TABLE 28-3 SNMP Properties (Continued)

Option	Functions for SNMP Properties
Settings	Pops up another dialog box in which the following options can be set. Polling Interval - sets the polling interval for the retrieval of the tables. By default, it is 5 seconds. Page Size (Rows) - sets the number of rows to be retrieved. No of Column View - sets the number of columns to be displayed in the SNMP Table - Panel. Default is 5 columns. Port No - sets the port number to which the request is made. SNMP version - allows selecting the desired versions of the SNMP. Retrieval Mode - sets the mode of retrieval for fetching the SNMP tables. By default, it is by GET NEXT. If the SNMP version is v2c or v3, GET BULK also can be used.
Start	Starts the retrieval of the table.
Next, Prev	Navigate the pages (rows) of the table.
StartPolling	Start polling of the table. Based on the polling interval value set in the settings option, it retrieves the table periodically.
StopPolling	Stop polling.
Refresh	When you don't use the polling option, click **Refresh** to refresh the table.
Add	Add a row to the table. Selecting this pops up another window through which the table values can be added.
Delete	Delete a row from the table.
Graph	Pops up a graph window and starts plotting the selected variable.
Original Table	Replaces the existing table data with the augmented table data. In a table, if one of the index columns is an external index, i.e., the index value is shared by some other table, and then the table is called an Augmented table. Augmented table comes into picture when there is a one-to-one dependency between rows of two tables. This situation might arise when a particular MIB imports another MIB and shares a single table. For example, ifXTable defined in IF-MIB is an augmented table, which has an external index ifIndex augmented from ifTable. Clicking the 'Augmented Table' button shows the columns of the table which augments the index from the original table.
Index Editor	Edit and set the index value of the table.

By right-clicking the table header (where the column name is displayed), a menu appears with the following options:

- *view column node details*
- *edit the header name of the selected column*
- *view Graph for selected cells*
- *add a new row to the table*
- *delete the selected rows from the table*
- *view the not-accessible index*

Using SNMP table, the SET operation for the table variables becomes easier. To set values for the table variables, the following steps need to be followed:

For creating a new row in a table, do the following:

1. In your MIB Module, include a table with RowStatus object defined.
2. Define a column in the table with SYNTAX RowStatus.
3. Load the MIB Module in the MibBrowser.
4. Select the table node from the tree and the table button on the toolbar. It displays the corresponding table.

5. Right-click the table header, and then select the *add a new row to the table* option. This displays a window for entering the values of the table.
6. Set the value for the column with RowStatus syntax to 4 for creating a new row, and then enter the values.

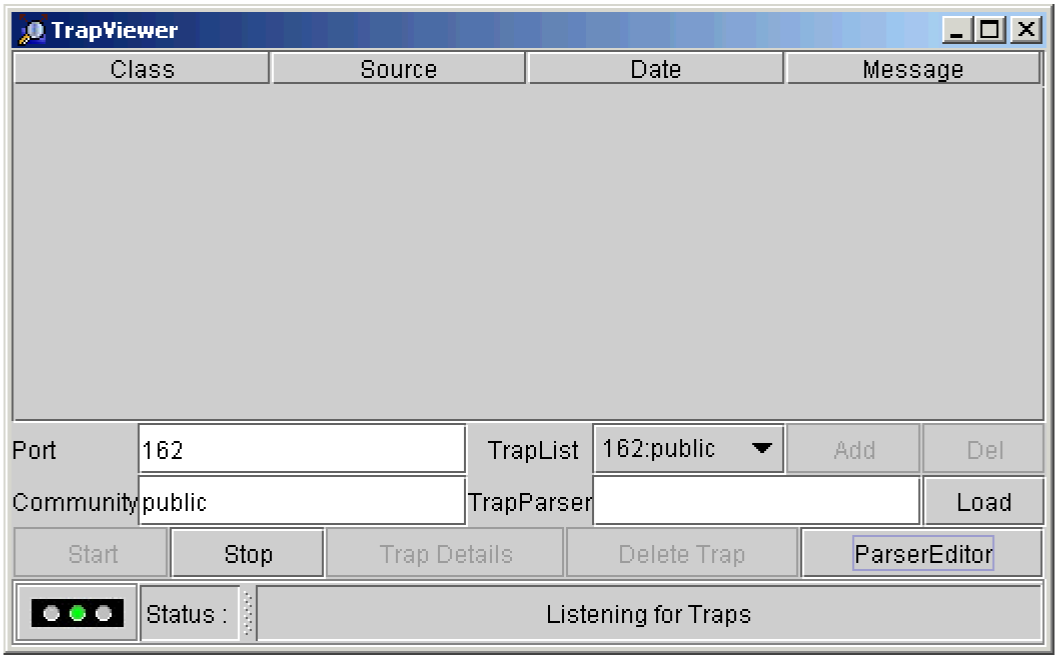
Note: If the RowStatus is not present in the table definition, then you can only modify the existing row by double-clicking the corresponding cell in the table.

7. Click **OK** after entering all the values.

28.7 Trap Viewer

Trap Viewer is used for receiving the traps. Using this you can view the incoming traps to the specified port. The traps can be sent from any host. The port number and the community name have to be set in the Trap Viewer. The trap originator should send the trap to the port number specified in the Trap Viewer.

The trap viewer is accessed using the *View -> Trap Viewer* menu option. This displays in a table format, as shown in the following figure.



Port 162

Community public

TrapList 162:public

TrapParser

Status : Listening for Traps

FIGURE 28-5 Trap Viewer

The trap viewer components are:

- Trap Table, in which the incoming traps are listed.
- A **Port** text field to specify the port on which the viewer will listen.
- A **Community** text field to specify the community of the incoming traps.
- A **TrapList** combo box, which contains the Port and Community list on which the trap has to listen.
- Field to load the Trap Parser file.
- **Start** and **Stop** buttons.
- Button to view the trap details.
- **Delete Trap** button to delete a trap from the Trap Table.
- Trap Parser editor.

The trap table has the following properties:

- Class - Defines the Severity of the Trap.
- Source - Displays the IP address of the source from where the trap was send.
- Date - Displays the date of receiving the trap.
- Message - By default, contains the VarBind list of the Trap, if any, else it is blank.

To view more details of the received trap, right-click a table entry and choose View Trap Details. Sorting of trap table columns is done by clicking the corresponding columns.

Trap Details shows more details about the incoming trap. Properties are shown in the following table.

TABLE 28-4 Trap Properties

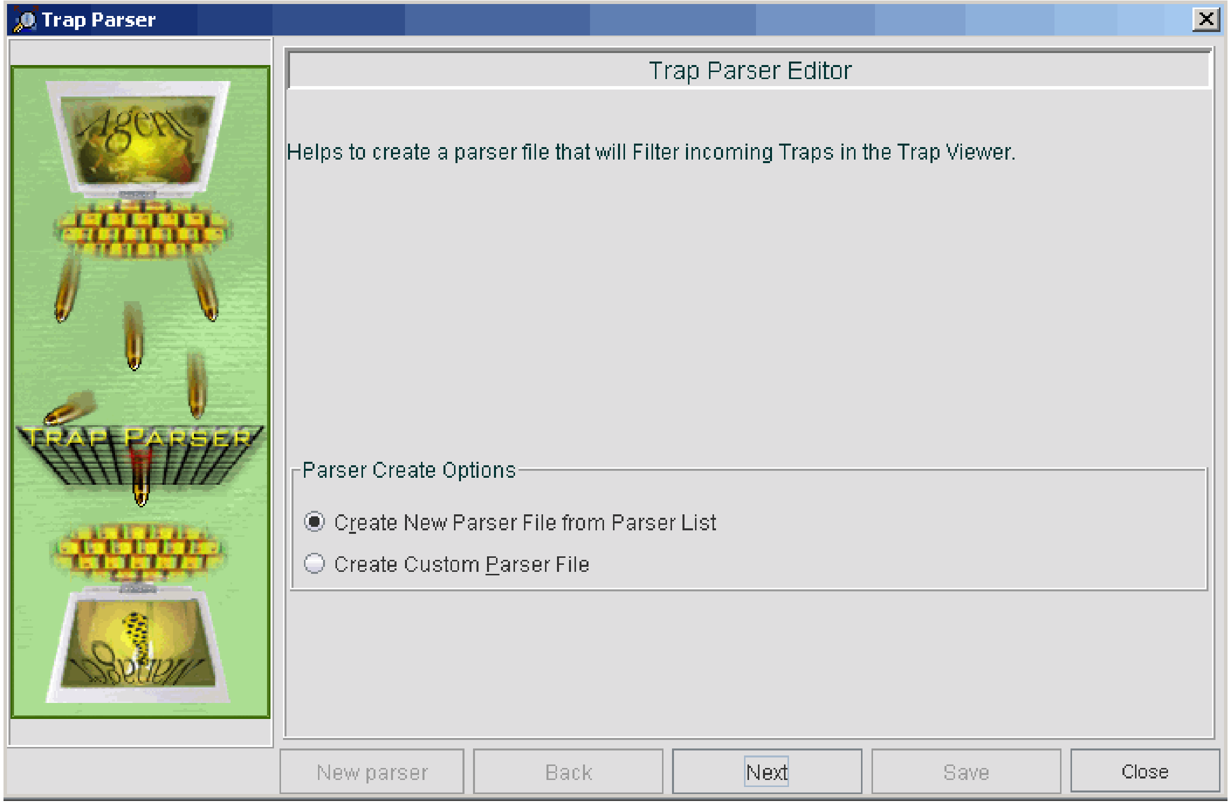
Property	Description for Trap Properties
Time Stamp	The Time Ticks value is converted into hours, minutes and seconds.
Enterprise	This field contains the enterprise OID.
Generic Type	This field can have values from 0-6, depending on the type of traps.
Specific Type	This field can have values from 1-64K.
Message	By default, this field will always contain the Varbinds in the Trap PDU. This can be substituted with text.
Severity	This field shows the severity of the trap. Default is Clear.
Entity	The source IP address from which the Trap originated.
RemotePort	The port on which the Trap was sent by the originator.
Category	Community string.
Domain	Source of the originator.
Network	The network (192.168.4.2) to which the device that generates the trap belongs.
Node	The device that generates the trap.
Source	The component or the element in the device that generates the trap.
Time Received	The time of receiving the trap.
HelpURL	Gives more details of the received trap. By default, the URL file name is <generic-type value> - <specific-type value>.html.

The Trap Viewer can filter incoming trap according to certain criteria called the Parser Criteria. The Trap Viewer shows only those traps that matches the Trap Criteria. The rest are dropped and is not shown to the user. The Criteria can be configured using the Trap Parser Editor.

28.8 Trap Parser

Trap Parser is a tool for creating trap parser files. The Trap Parser Editor is used to configure and parse the trap events. Since Traps typically contain cryptic information not easily understandable to the users, trap parsers are required to translate or parse traps into understandable information.

To view the Trap Parser Editor, click **ParserEditor** in the Trap Viewer window. Refer to the following figure. Use the Next button to view the options.



Trap Parser Editor

Helps to create a parser file that will Filter incoming Traps in the Trap Viewer.

Parser Create Options

● Create New Parser File from Parser List

○ Create Custom Parser File

FIGURE 28-6 Trap Parser Editor

Each incoming trap must have the Match Criteria to show the traps in the Trap Table.

You may enter any number of parser match criteria into a single parser file with a different parser name. The Trap Viewer looks for a match criterion sequentially. Thus, if a match is found for a received trap, the trap is shown on the Trap Table. Once the criterion is matched for a trap, an event is fired, which shows a trap entry in the trap table and further checking of match criteria in the loaded parser file is skipped.

While listening to traps, only one parser file can be loaded by the Trap Viewer. A parser file can have any number of match criteria to match. The Trap Viewer checks all the match criteria in a trap parser file until one is found.

The Match Criteria are:

- Generic Type - Each trap has a generic type number. This number must be specified for the trap parser and only when this matches, the trap parser be applied to a trap. The only exception is that when the generic field is left blank or filled with negative value, the trap is allowed to be parsed. The values for generic type ranges from 0 to 6.
  - 0 - cold start
  - 1 - warm start
  - 2 - linkdown
  - 3 - linkup
  - 4 - authentication failure
  - 5 - egpNeighbourloss
  - 6 is for enterprise specific
- Specific Type - This field can have values from 0-64k. When this field is to be matched, the Generic Type must always be enterprise specific.

- Enterprise OID - The enterprise field is the SNMP enterprise identifier in the trap, which is used to uniquely identify traps for a particular application. The parser is applied only when the trap enterprise field starts with the enterprise field you specify. The only exception is that when the enterprise field is left blank, the trap is allowed to be parsed.
- OID and Value - This extends the match criteria. There must be a match for all the OID:Value pairs (specified in the list box) in the Trap PDU of the receiving trap.
- Agent and Port - This also extends the match criteria. The trap must be sent by an Agent specified in the Agent:Port list box. If the Port is 0, then the source can send the trap from any port.

For each match criterion, a name is given called the Trap Name. The fields in the event details are configured in the Output Event Parameters section. Once the Trap is matched by the match criteria, the trap is added to the Trap Table. The Output Event parameters are shown as the Trap Details, which gives more specific information regarding the trap.

By default, some of the field of the Output Event parameters are filled by a variable called parser variables, usually starting with $. These variables substitute a specific characteristic of the parser in the Trap Details.

Values for field are:

- $Community - This token is replaced by the community string of the received trap.
- $Source - This token is replaced by the source name/address of the received trap.
- $Enterprise - This token is replaced by the enterprise ID of the received trap.
- $Agent - This token is replaced by the agent address of the received trap.
- $SpecificType - This token is replaced by the specific type of the received trap.
- $GenericType - This token is replaced by the generic type of the received trap.
- $Uptime - This token is replaced by the uptime value in the received trap.
- $* - This token is replaced by all the variable bindings of the received trap, including the OID and the variable values of each variable binding.
- $# - This token is replaced by all the SNMP variable values in the variable bindings of the received trap.
- $N - This token is replaced by the (N-1) SNMP variable value in the variable bindings of the received trap.
- @* - This token is replaced by all the OID values in the variable bindings of the received trap.
- @N - This token is replaced by the (N-1) OID value in the variable bindings of the received trap.

28.8.1 Procedure to Create a Parser File

1. Click **ParserEditor** in the Trap Viewer.
2. Enter the Match Criteria, which includes Trap Parser Name, Generic Type, Specific Type, Enterprise OID, OID and Value pair (optional) and Agent and port pair (optional). (The Generic Type - means, it will match any value for this field).
3. Click the OutPut Event Parameters tab and fill in the event parameters. These include Severity, Failure Object, Community, Node, Source, Help URL, Message, and Severity Color. If left blank, the following fields will default as follows:
   - **Community** - Name
   - **Node** - $Source
   - **Source** - $Source
   - **Help URL** - $GenericType-$SpecificType.html
   - **Message** - $*
4. Click **Add** to add the Trap parser to the Parser List.
5. Repeat from Step 1 to add more Match Criteria for incoming Traps.
6. Save the current parser criteria into a parser file using the **Save** button.
7. After saving, the parser file is displayed on the Parser File text field.

8. Close the Trap Parser Editor. A parser file is now created.

28.8.2 Adding a Trap Definition from MIBs to a Parser File:

1. Choose the MIB file (standard or any other) in the MIB File text field.
2. The setting of the MIB is automatically shown on the MatchCriteria and Output Event parameters sections.

If any modification is made after saving to a file, you must click **Mod** below the Trap list box, and then choose the same file from the **Save** option. This saves the modified information into the same file.

28.8.3 Filtering Incoming Traps

1. Create the parser file.
2. In the Trap Viewer window, load the parser file that is created.

Note: The parser files are saved with .parser extensions

3. Start the Trap Viewer. Now, the Trap Viewer will filter all the incoming traps according to the Match Criteria.

28.8.4 Setting Trap Parser Parameters

The following are some important fields and information on how to configure them for a given trap.

- name - The name of the parser.
- severity - This is used to specify the state of an event, which determines the severity shown in the ListTraps. This severity determines how a fault is affected by this event. The type of this filed is an integer ranging from 0 to 6.
  - 0 is for All.
  - 1 is for Critical.
  - 2 is for Major.
  - 3 is for Minor.
  - 4 is for Warning.
  - 5 is for Clear.
  - 6 is for Info. By default 6 will be assigned.
- textDefn - This is the message text seen for this event in the ListTraps and logs.
- categoryDefn - This is a type of the trap that can be used to categorize trap events.
- helpDefn - The associated document for this trap.
- ST - This is the specific type of the trap that has values from 0-64K.
- GT - This is the generic type of the trap that has values from 0-6.
- enterprise - This is the enterprise OID of the trap.

For example, you can try the following:

This command sends the trap using the sendtrap application (from the agent 192.168.1.1 at port 4001).

Input: java sendtrap -p 4001 -c public -m mibs/RFC-1213 192.168.1.1 .1.3.6.1.2.1.1.1.0 192.168.1.1 0 0 1000 .1.3.6.1.2.1.1.1.0 xyz

This matches the Match Criteria of the Trap Parser if it is:

- Generic Type - 0
- Specific Type - 0
- Enterprise oid - .1.3.1.6.1.2.1.1.1.0

- Oid - .1.3.6.1.2.1.1.1.0
- Value - xyz
- Agent - 192.168.1.1
- Port - 4001

The TrapParser gets trap from any trap originator and parses the trap event.

28.9 Graphs

The MIB Browser enables a real-time plotting of SNMP data on a graph. Currently, two types of graph are supported: line graph and bar graph. The SNMP data to be polled should be of integer or unsigned integer data type. Typically, the values that are plotted are of type Counter, Gauge, or Timeticks.

The steps listed below should be followed for plotting the SNMP data in the graph:

1. Ensure the appropriate MIBs have been loaded.
2. Specify the proper agent host name or IP address in the host field of the Mib Browser.
3. Specify a valid variable. The variable needs to be an integer or unsigned integer (Counter, Gauge or Timeticks). The variable can be chosen by browsing the MIB in the MibTree.

After selecting the variable from the MibTree, click the **GRAPH** icon or select the menu item Line Graph or Bar Graph from the View menu. This brings an automatically updated graph, showing the results of periodically polling the specified agent for the specified OID. By default, polling for the graph is done every 5 seconds.

The following options can be configured for the graph:

- Polling Interval - Default value is 5 seconds: editable, can be given any value.
- Average over Interval - By default, the graph shows the actual values of a variable for different hosts. In other words, the values of the specified OID are plotted for different hosts for the given polling interval. This option is used to take the average of the values at a given polling interval for plotting the graph.
- X axis scale - Allows to set the X axis scale; the minimum is 300 secs.
- Show Absolute Time - If selected, it shows the time in hrs:secs otherwise in seconds.
- Max X value - Allows to set the maximum time the graph can plot. The default maximum value is 3600 secs.
- Show Polled Values - If selected, it shows all the polled values in a particular time period. By default, it is disabled.
- Log File Name - The filename for the log file can be set here. By default, the log filename is graph.txt. If **Log Polled Values** is selected, all the polled values are logged in this file. This option is not enabled when the MibBrowser runs as an applet because of security restrictions.
- Log Polled Values - If selected, it logs the polled values. By default, it is disabled.
- Show absolute counters - To enable the plotting of the absolute value. By default, the graph plots only the difference between the two values.
- The **Stop** button can be used to stop the polling of the variable. The **Restart** button can be used to restart the polling. The Close button is used to close the graph window.

The Mib Browser can plot multiple graphs showing values for different variables from different hosts.

28.10 CWMP

The CPE WAN Management Protocol (CWMP) is a messaging protocol designed for communication between the CPE devices and the management system. Specifications for this protocol are written by The Broadband Forum (formally DSL Forum) in technical reports. The TR-069 specification defines the messaging format based on XML for communicating using CWMP.

Previously, the discovery process and all NMS-supported operations used CLI or SNMP to communicate with the devices. Now TR-069 operations can be performed on Comtrend CPEs and AT-iMG devices. Although not all operations are implemented, there is a generic TR-069 client application implemented that can be used to execute any of the operations described in the TR-069 specification.

To access this tool, select *Tools* > *CWMP Browser*. Refer to the following figure.

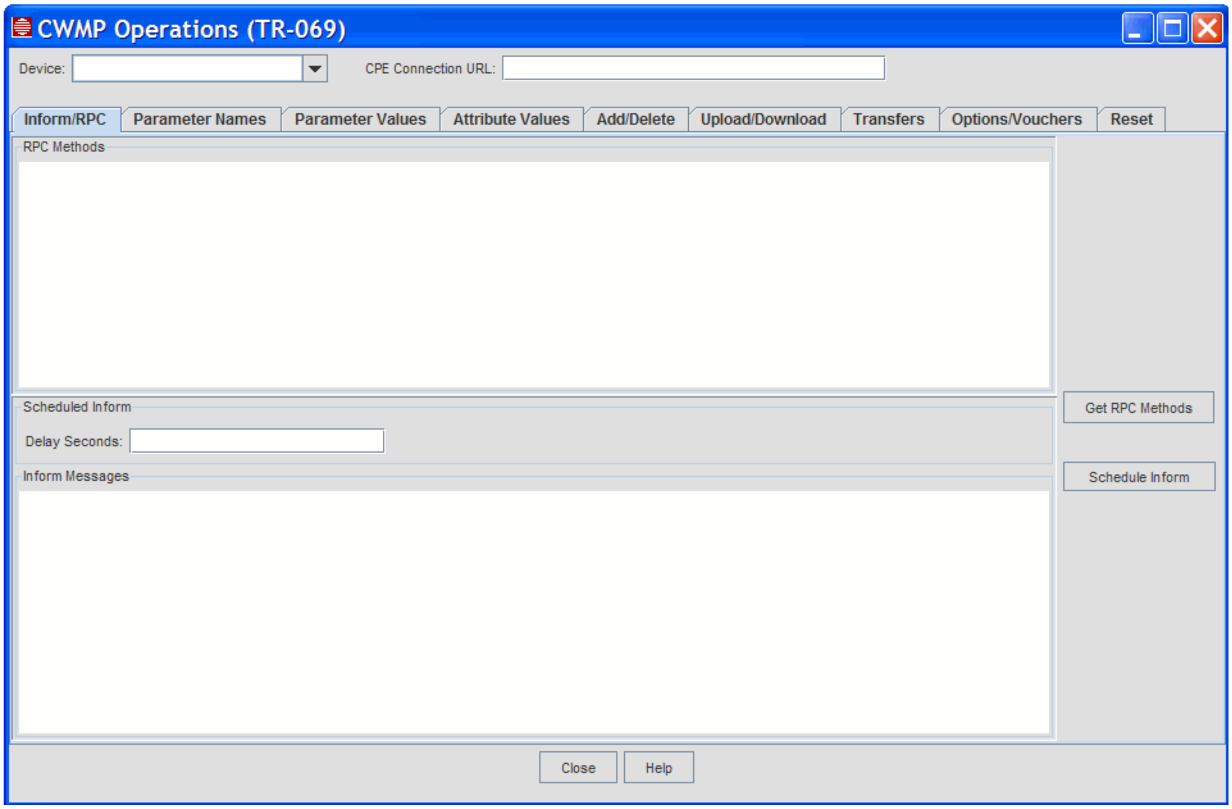


FIGURE 28-7 CWMP Browser - Initial Screen

.If any devices managed using TR-069 have been discovered using the NMS, they will appear in the Device pull-down. The Connection URL is the URL on the CPE the Auto Configuration Server (ACS) can use to initiate a connection. (This is done when using the Comtrend or RG Boot Configurator.) Also, the IP address of the ACS (the NMS being used) must be provisioned by accessing the device (using the client's browser, for example). Error messages may occur if these are not present.

The tabs and buttons follow the operations of the TR-069 specification.

29. Object Properties to Define Objects and Custom Views

With object properties, the user can perform these tasks:

- Define a specific object - The properties of an individual object are viewed and defined using the Managed Object properties form. Several of these properties are critical, since certain object properties allow the object to be discovered and therefore managed by the AlliedView NMS.
- Define a custom map view - When creating a custom map view, the user can define properties that filter the view according to a property criteria. Moreover, certain properties are specifically used to define a filter. For example, to create a map view that shows only Telesyn MAP devices, the user could use a number of criteria that would result in displaying the Telesyn set. Instead, the user only has to include the property **category** with the value *Telesyn* to the custom view to select only those devices.
- Define a custom table view - For objects that are listed in the table format, the user can define which properties will appear as columns and which criteria for properties will filter the view.

Caution: The user can delete as well as add Custom Views. This provides flexibility, but users should not delete any views unless they are sure that is what they wish, since some views require the combination of many properties.

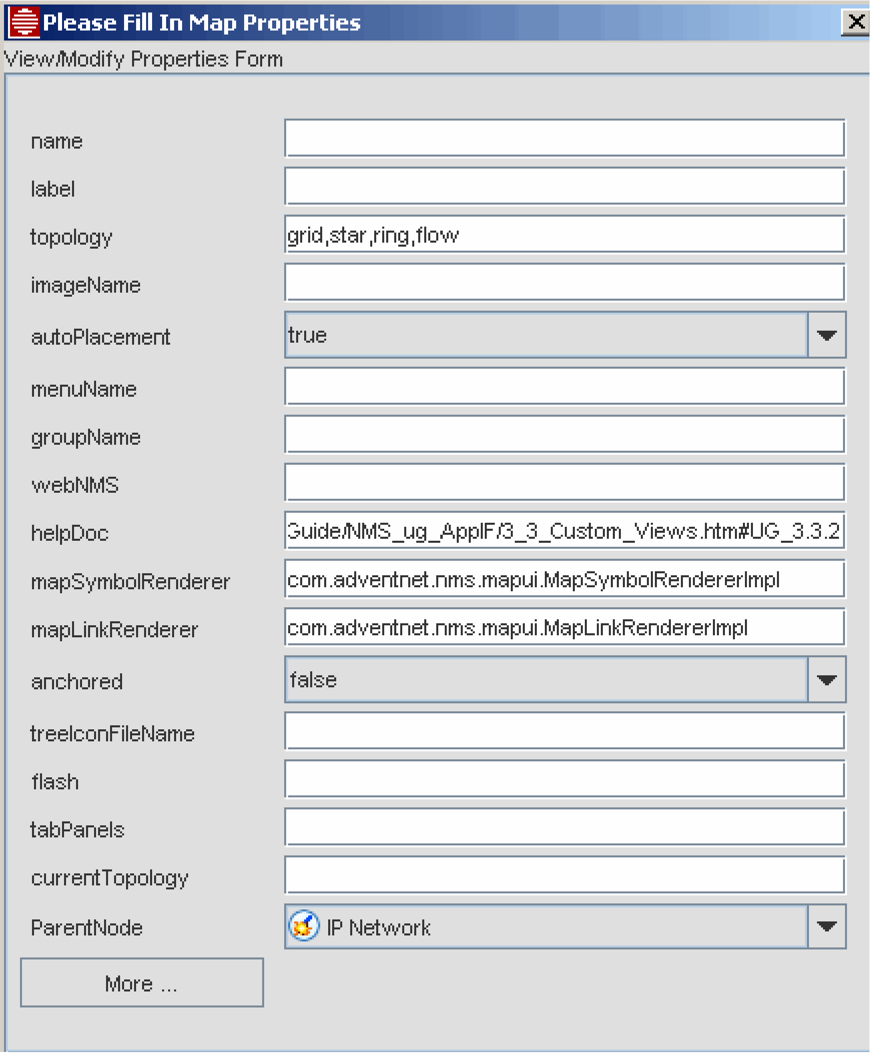
29.1 Defining Custom Map Views

29.1.1 Adding a Custom Map - Map Properties Forms

When creating a map, you have these options:

- Create a custom map (only those objects that meet a specific criteria can be included).
- Modify the map appearance for existing default maps or custom maps

To create a custom map, select *CustomViews > Add New Map* from the Panel-Specific Menu Bar, which brings up the following figure.



Please Fill In Map Properties

View/Modify Properties Form

name	
label	
topology	grid,star,ring,flow
imageName	
autoPlacement	true
menuName	
groupName	
webNMS	
helpDoc	Guide/NMS_ug_ApplF/3_3_Custom_Views.htm#UG_3.3.2
mapSymbolRenderer	com.adventnet.nms.mapui.MapSymbolRendererImpl
mapLinkRenderer	com.adventnet.nms.mapui.MapLinkRendererImpl
anchored	false
treeIconFileName	
flash	
tabPanels	
currentTopology	
ParentNode	IP Network

FIGURE 29-1 Add/Modify Map Properties Form

In the form, specify the set of map-related information before adding the map. The following table describes the various fields that you need to fill in the form.

TABLE 29-1 Map Properties

Map Property	Description of Map Properties	Example
label	The name that will be displayed in the panel and tree.	iMAP_only
topology	The permission layouts of the map. You can use comma separated values.	
imageName	The image file to appear as the background of the map. These are stored in <NMS Home>/Images	world.png
autoPlacement	A boolean that specifies whether the symbols on the map are placed automatically. The default is True.	

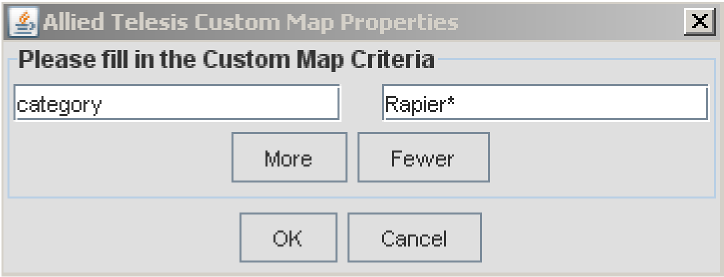
TABLE 29-1 Map Properties (Continued)

Map Property	Description of Map Properties	Example
menuName	The panel-specific menu file for this map. The menu files are in the <NMS Home>/mapdata/menus directory.	
mapSymbolRenderer	The renderer that paints the map symbols in the map canvas. By default, there are three map symbols renderers included with the product.	
mapLinkRenderer	The renderer that paints the links in the map canvas. By default there are two map link renderers included with the product.	
anchored	A boolean that specifies whether the anchor property of the map is True or False. If True, the map becomes non-editable (cannot add mapclient components). If False, the map is a normal editable map. The default is False.	
treeIconFileName	The name of the icon file that appears in the client tree against the map node.	
currentTopology	The layout to apply to default of this map. If you do not specify one, the first entry of the topology field is the default. If you do not specify anything in the topology field, then NMS uses the flow layout by default.	
ParentNode	The name of the of the parent node in the tree. For example, if you specify the parent node as “Fault” then the map is added under the Fault Node in the tree.	

Once you have filled in the map properties, click **More**, and the UI shown in the following figure will pop up. In this UI, you can specify a Managed Object and the criteria that will filter what will appear in the map. Note that the match criteria can only be the properties of the managed object.

Caution: The property name on the left is case-sensitive. Property names usually have medial capitalization ("camel-case"), for example ipAddress. If you enter the case incorrectly, no criteria will be used, and the new map will contain all managed objects in your network. For the correct property name to use, refer to the tables in Section "Managed Object Properties and Custom Views" on page 1063.

Note: The property value on the right may contain the wildcard character "", and may contain comma separated values, for example "10.1.1.*, 10.1.2.*". For more information, refer to Section "Matching Criteria" on page 1059.*


Allied Telesis Custom Map Properties
Please fill in the Custom Map Criteria
More
Fewer
OK
Cancel

category

Rapier*

FIGURE 29-2 Adding Managed Object Criteria to Map View

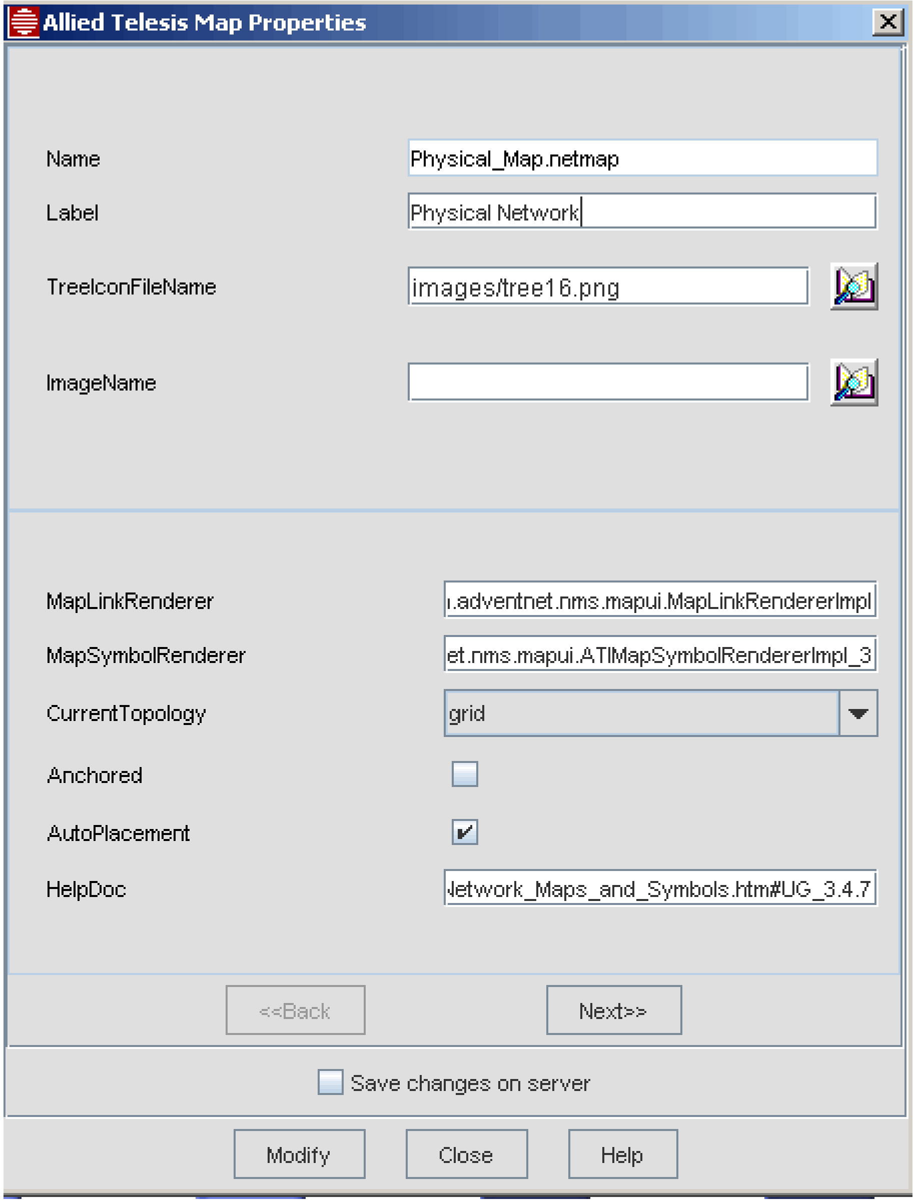
Click the **Add Map** button to add the map. The new map will appear in the tree.

Note: The properties for an object type can be applied for both the Map and Table Custom Views; for example, the properties/ criteria for routers can be applied for both routers as a map node and routers in the network inventory. Therefore, to see which properties apply for a map node object, refer to the table for the same object for a table view.

To change the map properties for an **existing** map, the user can double-click in a blank area. This brings up the **Map Properties** form, as shown in the following figure.

Note: If you double-click a blank area for the Physical Network, the Layer 2 links form appears. If you wish to change the appearance of a map with physical devices, select View -> Details with no devices selected.

Note: The tic box Save changes on server makes the change so that all users will see the same changes.



Name	Physical_Map.netmap
Label	Physical Network
TreeIconFileName	images/tree16.png
ImageName	
MapLinkRenderer	ı.adventnet.nms.mapui.MapLinkRendererImpl
MapSymbolRenderer	et.nms.mapui.ATIMapSymbolRendererImpl_3
CurrentTopology	grid
Anchored	□
AutoPlacement	☑
HelpDoc	Network_Maps_and_Symbols.htm#UG_3.4.7

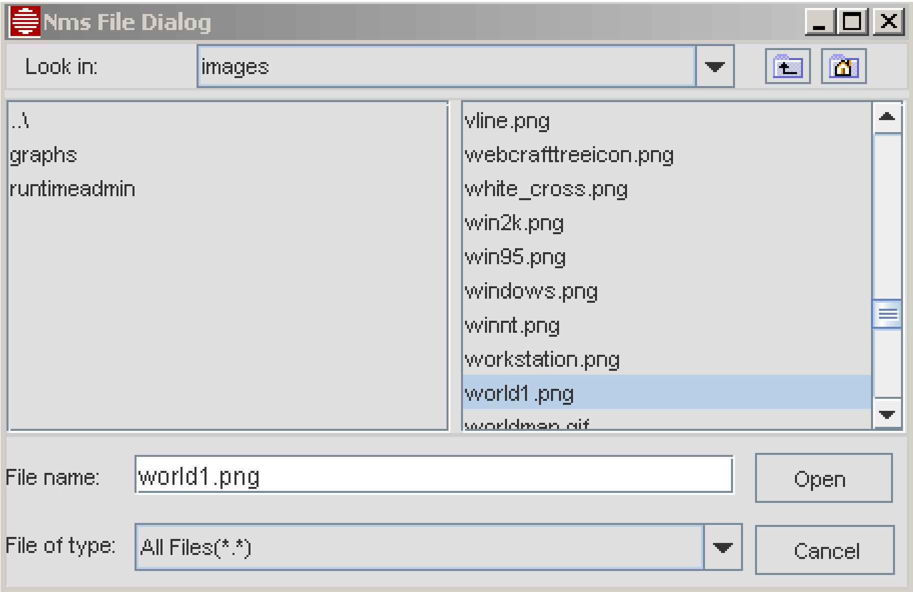
□ Save changes on server

FIGURE 29-3 Map Properties Form

29.1.2 Example - Change a Background Map

An example for Map Properties is to change the background map for the Physical Network node. Following are the steps:

1. Go to the Physical Network node and select *View -> Details*. The **Map Properties** form appears.
2. Images are stored in <NMS home>/Images. (You can add other images to this directory.) Click on the ImageName book icon in the **Map Properties** form and select an image file, as shown in the following figure.



Look in: images

File name: world1.png

File of type: All Files(*.*)

FIGURE 29-4 Selecting a Background Image for a Map

3. Click on **Open**, and then **Modify** on the Map Properties form. The image becomes the background image for the map.

29.1.3 Example Custom Map for iMAP Devices Only

Following are the steps to create a custom map of Allied Telesis devices.

1. From the Physical Network Map choose *Custom Views -> Add New Map*. The View/Modify Properties Form (See Figure 29-1) appears.
2. In the form, fill in a name (such as *iMAP_only*) and label (also *iMAP_only*).
3. Click on **More** to bring up additional Map criteria.
4. Enter the property **category** with the pre-defined value *Telesyn*.
5. Click **OK**, and on the Properties form click **Add Map**.
6. There is now a Custom Map that shows only Allied Telesis iMAP-type devices. Refer to Figure 29-5.

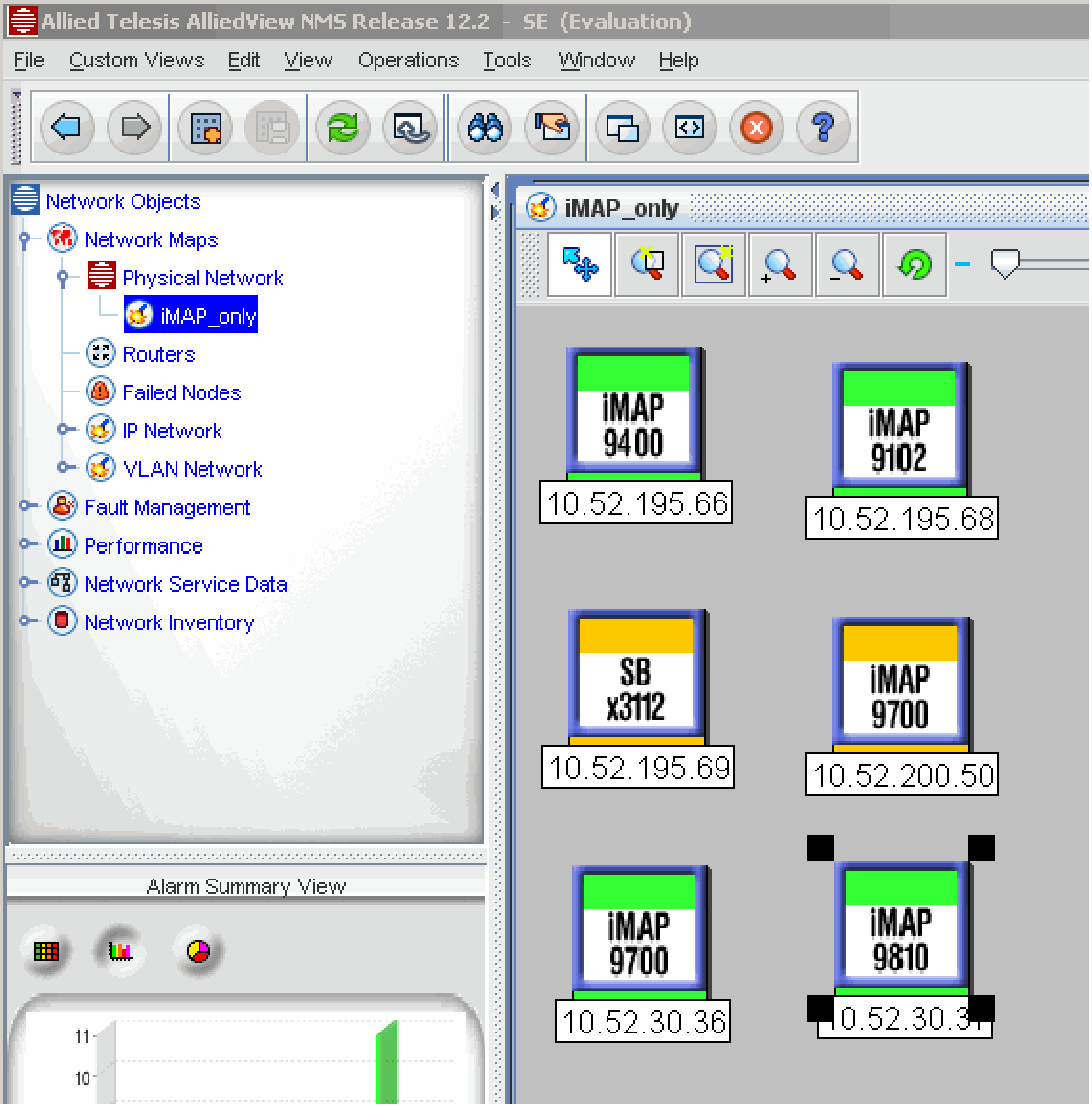


FIGURE 29-5 Example Custom Map for Telesyn devices

29.2 Using Object Properties

A custom table view is an option to view a subset of data that meets a certain criteria from the larger collection, such as Events or Alarms. You can use custom views to narrow the range of items, which allows an easier search.

Custom views have the following special features:

- A view can be created to match a specific criteria.
- Views are updated dynamically.
- The same custom view can be used at different levels.
- The column (properties to view) can be customized
- Column order and sorting of data can be saved these in the custom view.
- Custom views can be modified and renamed.

To create a custom view, you first define the criteria for the view, and then specify how to view the filtered data. The options for custom views are as follows:

- Add/Modify the Custom View

  When creating a custom view, the user fills out a Specify Event Filter Criteria form, which contains Properties and Tree Node Properties. Once created, the view can be seen in the node tree on the left. The user can then select the view and modify the criteria if need.

- Remove Custom View

  The user can select the view in the NMS Tree and choose *Remove Custom View* from the either the Panel-Specific Menu Bar or from the pop-up menu accessed by a right clicking the view in the tree. This option will remove the view form the tree.

- Save Custom View Data

  After sorting and selecting a range of items, the user can save that specified list by selecting *Save Custom View State* from the either the Panel-Specific Menu Bar or from the pop-up menu accessed by a right clicking the view in the tree.

29.2.1 Objects for Table Views

This section lists the property details of the objects that make up the AlliedView NMS. The following table lists the objects that have properties and which subsection describes these properties.

Note: To filter on iMG/RGs, refer to the AlliedView NMS Administration Guide.

.

TABLE 29-2 Tree Node Properties - Reference Table

Object	Reference
Network	"Networks" on page 1063
Device (Node)	"Devices (Nodes and Routers)" on page 1065
Customer Port	"Customer Ports" on page 1068
IP Interface (IP)	"Interfaces (IP)" on page 1069
Profile	"Profiles " on page 1071
Vlan Interface (VIF)	"VLAN Interfaces " on page 1072
Physical Links	"Physical Links" on page 1074
PMs	"Performance Monitoring" on page 1075
Events	"Events" on page 1077

TABLE 29-2 Tree Node Properties - Reference Table

Object	Reference
Alerts	"Alarms" on page 1080
Links	"Adding Links to Existing Custom Physical Map" on page 1083

29.2.2 Matching Criteria

Points to consider in regards to using properties are as follows:

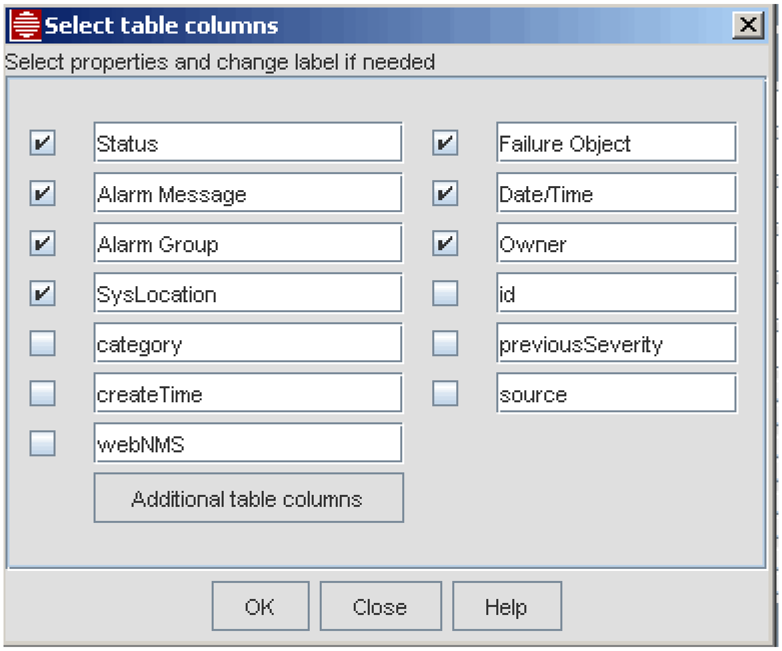
- Most of the Properties listed while adding a custom view are string based. Additionally, if there is a Boolean, the properties form indicates a choice box, containing three items: all, true, and false. Selecting all will amount to the property not being taken into consideration. Selecting true or false will have the expected behavior.
- For string-based properties, the string value is absolutely matched. For example, the string "Router" matches the exact word only.
- The wildcard '*' (asterisk) is supported to replace one or more characters. For example, if you want to view objects whose names start with 'sa', then you have to specify it as 'sa*'. Similarly, if you want to view objects whose names end with 'com', then you have to specify as '*com'.
- Wildcard, '?' is not supported and is treated just as an ordinary character.
- For specifying multiple criteria for the same property, separate them with a comma. For example, if you want to view objects named nms-server1, nms-server2 and nms-server3 then specify as nms-server1, nms-server2, nms-server3.
- Status, Severity, etc. are also treated as strings. Therefore, for a filter of Alarms, with severity critical, specify 'crit*".
- To exclude certain items, as part of the filtering criteria, append a '!' before it. The exclamation mark should be used to ignore those values. For example, if you want to view objects, which do not start with 's", then specify the property as '!sa*' or if you want to see all Alarms, except those with severity other than warning and clear, then any of the following will work:
  - !war*, !cle*
  - !warning, !clear
  - cr*, maj*, mino*
  - critical, major, minor
- In the Alarms and Events panel, filtering based on time can be done by specifying the starting time and the ending time. The formats in which the time is to be specified are as follows:
  - MON DD,YYYY HH:MM:SS AM/PM (For JavaUI) for example, Oct 27,2002 12:24:12AM and
  - MONTH DD,YYYY HH:MM:SS AM/PM (For JavaUI) for example, Oct 27,2002 12:24:12 AM. (The incompatibility is due to different JVM versions on Client and Server sides).
- In the Network Inventory view, the properties form initially contains only properties common to all Managed Objects. But the properties form changes to display properties specific to the particular object on double-clicking the desired property. That is, after viewing the properties of an interface, on double-clicking that, the properties specific to the interface are displayed (IfIndex, IfSpeed, etc.) which are part of the properties form.
- It is advisable to leave the fields blank that are not necessary but are part of the filtering criteria.
- Once the filtering criterion is specified, you can optionally give the filter a name and then select the ApplyFilter option. The client then sends a request to the server to filter the objects while it adds the name of the filter to the tree in the main panel.

- The time to filter may vary, depending on the total number of objects, the complexity of the filter criteria, and the mode of storage.
- Custom Views, once created, continue to be updated and navigable for additions/deletions till the client is closed or the custom view is removed using Remove Custom Views option.

Note: *Use the Custom Views with caution and remove the unnecessary ones. This allows quicker updates and clearing of resources associated with each Custom View, both on the client and server side.*

Note: *If all the above parameters (except filter view name) are left blank, then the default value all is assigned. For Date/Time properties by default will show the current date and time, requires data in the order of month, date, year, hour, minute, second and AM / PM which can be chosen by using the up and down arrows.*

In the properties form, you can also click **Select Props to View**, which opens a window with the default properties to be shown in the selected table (as shown in the following figure).



Select properties and change label if needed

☑ Status
☑ Alarm Message
☑ Alarm Group
☑ SysLocation
□ category
□ createTime
□ webNMS
☑ Failure Object
☑ Date/Time
☑ Owner
□ id
□ previousSeverity
□ source

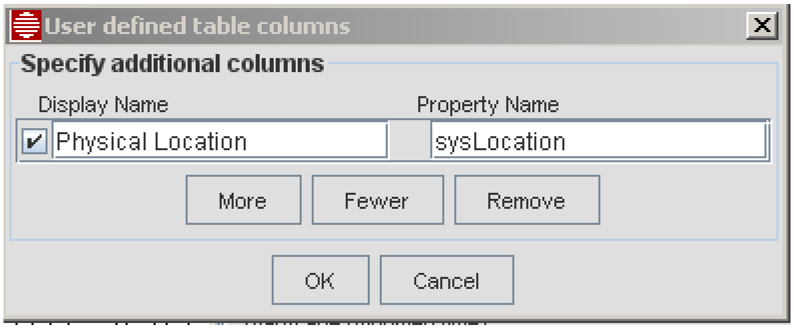
FIGURE 29-6 Selecting Properties to View in a Custom View

Clicking the **Additional table columns** button in this **Select Table Columns** form brings up the **User defined table columns** form. In this form the user can enter the user properties that were defined in the Event Parser and what the displayed table column will be.

Note: *If additional user properties have been added, they can be included here by using the More button and entering them in the Property Name field. The More button can also be used to add any properties that are expected to be added in the future.*

Figure 29-7 shows the User defined table columns with the property sysLocation filled in.The column display will be Physical Location.

Note: *The Location Names are defined as part of provisioning device information.*


User defined table columns

Specify additional columns

Display Name	Property Name
☑ Physical Location	sysLocation

FIGURE 29-7 Adding Properties to a Network Custom View

Clicking the **Additional Criteria** button in the **Show objects with these Properties** form brings up the **Criteria dialog** form. In this form additional criteria can be specified for both the NMS properties and any user properties (including sysLocation).

Click **Apply Filter** to see the resulting view. To save, right-click on the node icon in the NMS Tree, and then select *Custom Views->Save Custom View State* from the pop-up menu.

29.2.3 Default User Properties Added by the NMS and Custom Views

To view information for the devices, user properties have been added to the tree node tables that show relevant information. When the NMS is first configured, they are grouped as follows:

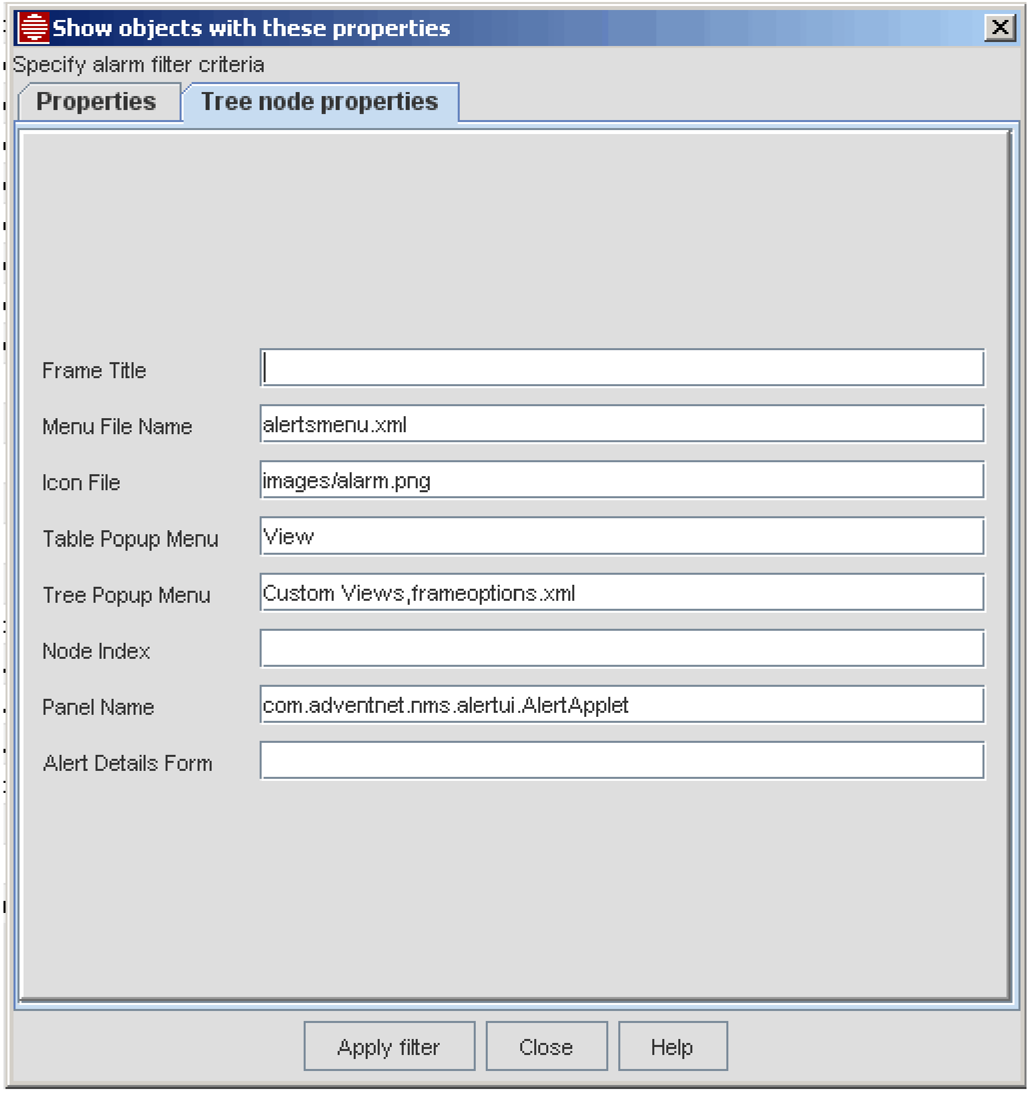
- Alarms – sysLocation
- Network – discover
- Nodes - SerialNumber
- Ports – customerID, ethIfIndex, portType, deviceID, adslIfIndex, slotID, portID
- VLAN Interface – parentkey, vlanparentnetwork, valnuntaggedports, vlantype, vlaninterfacevid, vlantaggedports
- Physical Links – Snode, DNode, DPort, SPort

These properties show up by default when the NMS is first configured, and the user can change the displayed column name if desired, in either the default view or a Custom view.

Caution: Although in the default View or Custom View these properties can be made not to display, the user should not do this since these properties were created to provide relevant information about a component. For example, for Physical links, the DPort property (Destination Port) would need to be shown to understand the configuration. These properties are therefore useful when creating custom views. However, even if a property is not displayed, a criteria can be set for the view based on that property.

29.2.4 Tree Node Properties Tab

The Tree Node Properties form determines the way the subset of data is presented for a View. This is done by selecting the Tree Node Properties tab of the Show objects with these Properties form, as shown in the following figure.


Show objects with these properties
Specify alarm filter criteria
Properties
Tree node properties
Apply filter
Close
Help

Frame Title	
Menu File Name	alertsmenu.xml
Icon File	images/alarm.png
Table Popup Menu	View
Tree Popup Menu	Custom Views,frameoptions.xml
Node Index	
Panel Name	com.adventnet.nms.alertui.AlertApplet
Alert Details Form	

FIGURE 29-8 Tree Node Properties Form for Events

The following table lists the properties.

TABLE 29-3 Tree Node Properties

MO Form Property (Label)	Description for Tree Node Properties
Frame Title	The information to be displayed on the title bar of the Custom View's internal frame is specified here.
Menu File Name	The panel-specific menu's file name is given here. If you have not specified this then the default menu is displayed.
Icon File	The icon to indicate the custom view is taken from this property. This icon is visible in the tree as well as in the title bar of the internal frame.
Table Popup Menu	The menu filename for displaying a contextual menu for the objects displayed in the table of the newly added custom view.

TABLE 29-3 Tree Node Properties (Continued)

MO Form Property (Label)	Description for Tree Node Properties
Tree Popup Menu	The menu filename for displaying a contextual menu for the newly added custom view node in the client tree.
Node Index	The position of the this new custom view in the node tree when this view is added as a child to an existing view that already has one or more child nodes. If the value is not entered, then the custom view is appended.

29.3 Managed Object Properties and Custom Views

The following tables list the properties for the various objects controlled by the AlliedView NMS. The columns of the table are as follows:

- **Form Property** - This is the property as shown on the Managed Objects Form. If an object is usually not changed by the user, **(Internal only)** is included.
- **Description** - This describes the property in detail.
- **Custom View Property** - If the property is used for a custom view, it is included here. Note that the spelling can be different. This is the **exact** spelling you must use when adding a property.
- **Examples for Custom View** - When setting a criteria for a property in a custom view, the example gives a typical value and explains how that value filters the custom view.

Note: An object may have many properties, but only a few that are commonly used for creating custom views; moreover, many properties are for internal reference and should not be changed. Therefore, these tables only include form properties that are useful for network administrators. These properties may be those included with the form or those that can be added with the More button.

29.3.1 Networks

29.3.1.1 Properties

The following table lists the properties for a network node. All the properties can be viewed by using the **Next** and **Back** button at the bottom of the form.

TABLE 29-4 Properties for Network Objects

MO Form Property	Description for Network Objects	Custom View Property (input this text)	Examples for Custom Views
Name	The device name, which is a unique name that is used as the key in the database. **This name cannot be changed.**	name	172.16.33.0 **Note: The name for a device should not include an '&' or Rediscovery will fail.**
DisplayName	The name by which the device is identified on the Graphical User Interface (GUI).This is intended to be more intuitive regarding the identification of the network, whereas the name can be any string with the only constraint being that it is unique.	displayName	Site_A (This would assume the network was contained in Site_A)

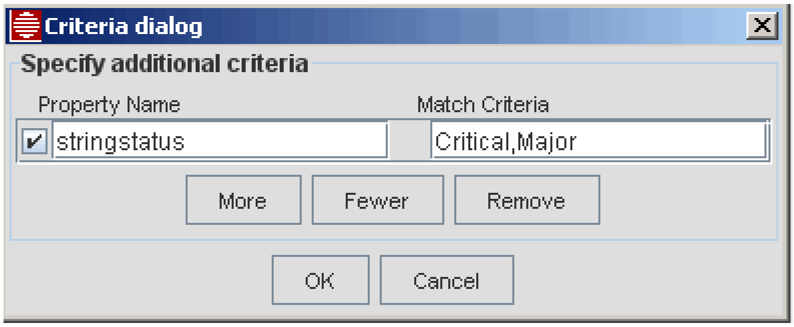
TABLE 29-4 Properties for Network Objects (Continued)

MO Form Property	Description for Network Objects	Custom View Property (input this text)	Examples for Custom Views
Type	The type of the object, such as whether it is a network, node, or an interface object, or something user specified, like router, switch, etc.	type	Network (In a network view, this would be the default, in other views this would set the criteria as showing only networks)
Managed	A checkbox that indicates whether the managed object is managed by the NMS. When checked, the object is being managed by the NMS. Otherwise, it is not.	managed	true (rather than a checkbox)
IpAddress	The IP address assigned to the object.	ipAddress	172.16.33.0 (This would be for the network)
InterfaceList	The interfaces contained within the network. In the Properties form this is a drop down list.	InterfaceList	172.16.33.20 172.16.33.21 The value **all** would select all nodes.
NodeList	The devices contained within the network. In the Properties form this is a drop down list.	NodeList	172.16.33.20 172.16.33.21 The value **all** would select all nodes. The DNS name can also be used.
DiscoveryStatus	The current status of the discovery process. The possible values are as follows: 1 = YET_TO_BEGIN - Discovery of network yet to begin. 2 = IN_PROGRESS - Discovery if network is in progress. 3 = FINISHED - Discovery of the network is finished. 4 = DISCOVERY_DISABLED - Takes this value if either discover is 'false' or managed is 'false' for this network.	DiscoveryStatus	2
StatusPollEnabled	A boolean that indicates whether the object status polling has been enabled for the object. It is set to true if status polling is enabled for the object, false otherwise.	DiscoveryStatus	
Tester	The type of testing to run when checking the status of the device.	DiscoveryStatus	
(More...)		subNets	172.16.33.20 172.16.33.21 (The value **all** would select all nodes.)
(More...)		stringstatus	Critical Major Minor Clear (separated by comma when choose more than one)

29.3.1.2 Custom View for Networks Example

If there are a large number of networks being managed, the user can create a view that shows networks in a Critical or Major state. In the Custom View form, the user would:

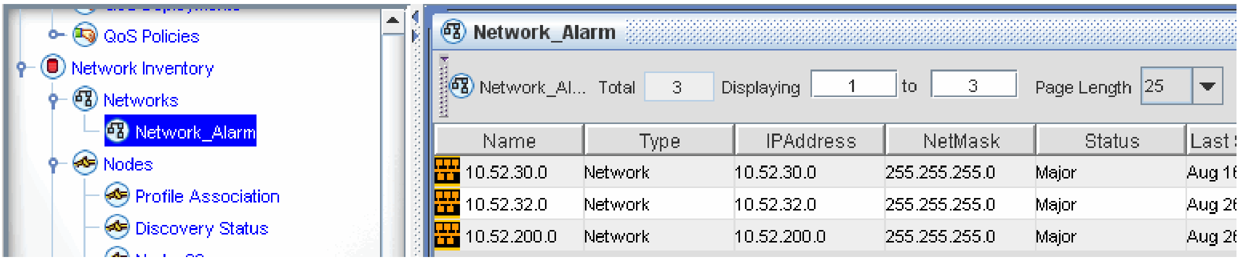
1. Select the Network node in the Inventory view and right-click *Custom View -> Add Custom View*.
2. In the **Filter View Name** field, type Network_Alarm
3. Click **Next** to access the **Additional Criteria**, and type in *status* and *Critical,Major*, as follows.



Specify additional criteria

Property Name	Match Criteria
☑ stringstatus	Critical,Major

4. Click on **OK**, and a network_alarm view is formed that shows only networks with a critical or major alarm. Refer to the following figure.



Network_Al... Total 3 Displaying 1 to 3 Page Length 25

Name	Type	IPAddress	NetMask	Status	Last
10.52.30.0	Network	10.52.30.0	255.255.255.0	Major	Aug 1
10.52.32.0	Network	10.52.32.0	255.255.255.0	Major	Aug 2
10.52.200.0	Network	10.52.200.0	255.255.255.0	Major	Aug 2

FIGURE 29-9 Customer View for Networks

29.3.2 Devices (Nodes and Routers)

29.3.2.1 Properties

The following table lists the managed object properties for Node devices. All the properties can be viewed by using the **Next** and **Back** button at the bottom of the form.

Note: The classname for Nodes is !RgMO (not RG devices) and this should not be changed..

TABLE 29-5 Managed Object Properties for Nodes

MO Form Property	Description for Nodes	Custom Map View Property (input this text)	Example
Name	The device name, which is a unique name that is used as the key in the database. **This name cannot be changed.**	name	172.16.33.11
DisplayName	The name by which the device is identified on the GUI.This is intended to be more intuitive regarding the identification of the device, whereas the name can be any string with the only constraint being that it is unique.	displayName	Building_A (This would assume the device was contained in Building_A)

TABLE 29-5 Managed Object Properties for Nodes (Continued)

MO Form Property	Description for Nodes	Custom Map View Property (input this text)	Example
Type	The type of the object, such as whether it is a network, node, or an interface object, or something user specified, like router, switch, etc.	type	9700 9400 Rapier* (all Rapier devices) RG* (all RG devices)
managed	A pull-down that indicates whether the managed object is managed by the NMS. When True, the object is being managed by the NMS. When False, it is not. When all, it includes all devices.	managed	true (would not include devices that were discovered and unmanaged)
IpAddress	The unique address assigned to each and every object.	ipAddress	172.16.33.11
netmask	The netmask that is specified for this managed object. Network masking is a methodology by which the elements in a network can be meaningfully categorized.	netmask	255.255.255.0
ParentNet	The ID of the network that contains this node or a list of network numbers if this is a router connecting two or more networks.	parentNet	172.16.33.0
InterfaceList	A non modifiable drop-down list of all interfaces on this device.	InterfaceList	172.16.33.20 172.16.33.21 (The value **all** would select all nodes.)
SysDescr	The value of the system description associated with the type of managed object to be filtered.	sysDesc	Telesyn 9700 all
SysOID	The system object identifier of the device as reported by the SNMP agent of the device.	sysOID	.1.3.6.1.4.1.207.1.15.3
Login	The CLI username to use when NMS executes CLI commands on the device. It is defaulted but it should be changed.	login	officer
Password	The password to use when NMS logs in with the CLI username.	password	nms_user
SysLocation	A string value to identify where the device is located	sysLocation	Building_A (This would assume the device was located in Building_A)
Category	The family of the device	category	Telesyn (includes all MAP devices) Rapier* (all Rapier devices) RG* (all RG devices)
SysContact	A string to identify the owner of the device	sysContact	Company_A

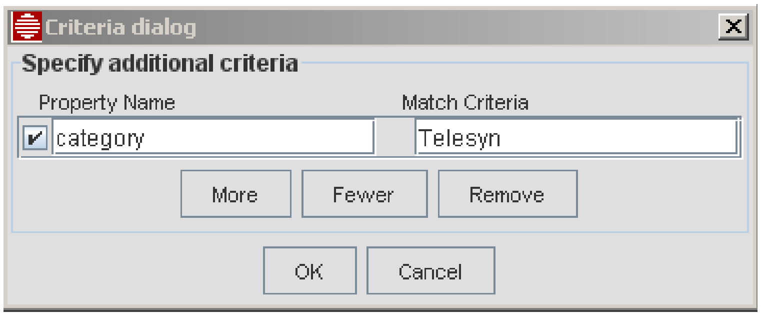
TABLE 29-5 Managed Object Properties for Nodes (Continued)

MO Form Property	Description for Nodes	Custom Map View Property (input this text)	Example
LastBackupTime	The time of the last backup performed for this device via the Device Backup/Restore MDTI Operation.	lastBackupTime	Wed Aug18 2010*
status (pull-down)		stringstatus	Critical,Major,Minor, Clear (separated by comma when choose more than one)

29.3.2.2 Custom View for Device Example

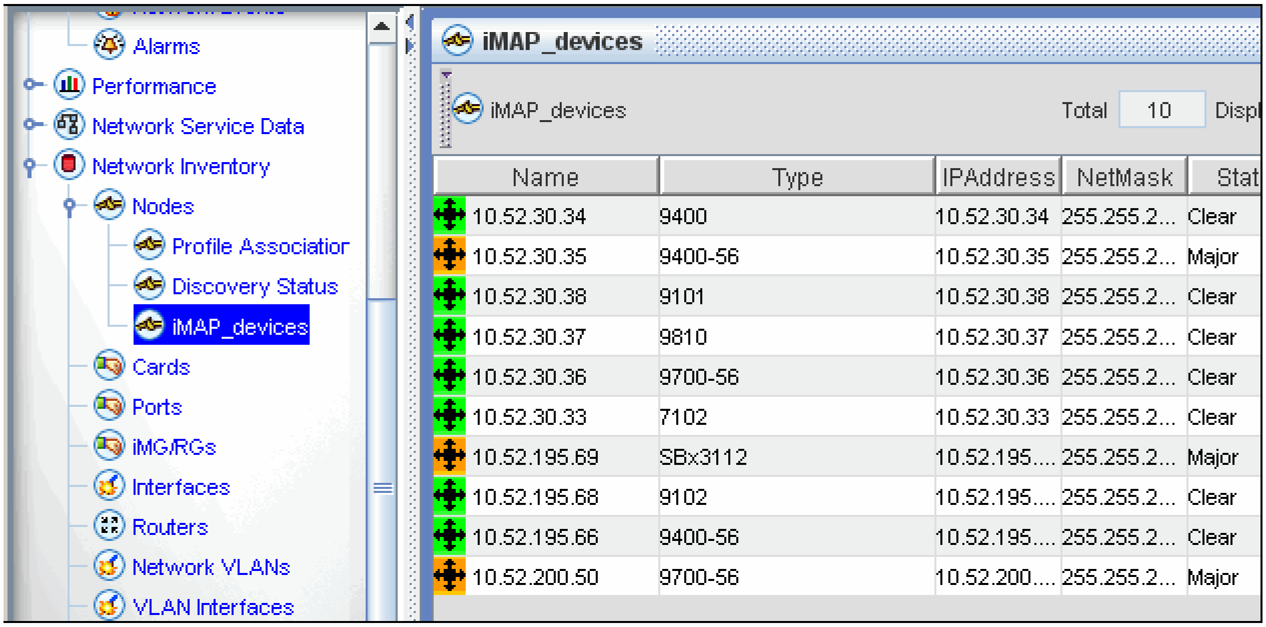
If there are a large number of nodes being managed, the user can create a view that shows only iMAP devices. In the Custom View form, the user would:

1. Select the Nodes in the Inventory view and right-click *Custom View -> Add Custom View*.
2. In the **Filter View Name** field, type *iMAP_devices.*
3. Click **Next** to access the Additional Criteria, and type in *category* and *Telesyn*, as follows.



	Property Name	Match Criteria
☑	category	Telesyn

4. Click on **OK**, and a iMAP_devices view is formed that shows only Allied Telesis Map devices, as follows.



iMAP_devices Total 10 Displ

Name	Type	IPAddress	NetMask	Stat
10.52.30.34	9400	10.52.30.34	255.255.2...	Clear
10.52.30.35	9400-56	10.52.30.35	255.255.2...	Major
10.52.30.38	9101	10.52.30.38	255.255.2...	Clear
10.52.30.37	9810	10.52.30.37	255.255.2...	Clear
10.52.30.36	9700-56	10.52.30.36	255.255.2...	Clear
10.52.30.33	7102	10.52.30.33	255.255.2...	Clear
10.52.195.69	SBx3112	10.52.195....	255.255.2...	Major
10.52.195.68	9102	10.52.195....	255.255.2...	Clear
10.52.195.66	9400-56	10.52.195....	255.255.2...	Clear
10.52.200.50	9700-56	10.52.200....	255.255.2...	Major

29.3.3 Customer Ports

29.3.3.1 Properties

The following table lists the properties for customer ports. All the properties can be viewed by using the **Next** and **Back** button at the bottom of the form.

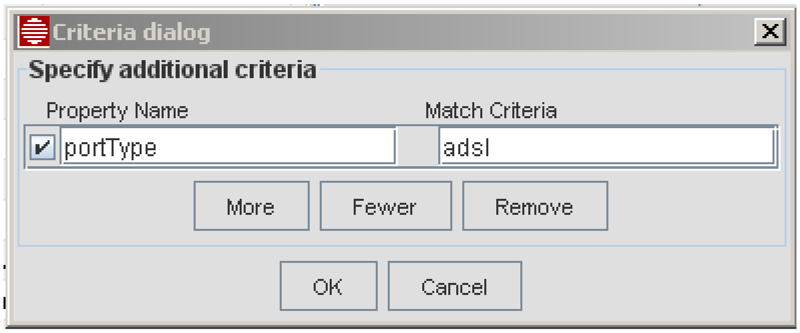
TABLE 29-6 Managed Object Properties for Customer Ports

MO Form Property	Description for Interfaces	Custom Map View Property (input this text)	Example
Name	The port name, which is a unique name that is used as the key in the database.	name	172.16.33.11_17.4 (This follows the device_card.port format)
DisplayName	The name by which the device is identified on the GUI.This is intended to be more intuitive regarding the identification of the device, whereas the name can be any string with the only constraint being that it is unique.	displayName	172.16.33.11_17.4
Type	The type of the object, such as whether it is a network, node, or an interface object, or something user specified, like router, switch, etc.	type	CustPort
CustomerID	The description from the “Show Port” CLI command.	customerID	x908_mgmt (or telephone number, a convenient way to identify the customer)
DeviceID	The device to which the port belongs	deviceID	172.16.33.11
PortType		portType	ADSL
EthIfIndex	An index number assigned by the NMS to identify the port and its type	ethIfIndex	112
PortProfileName	The profile used on the port	portProfileName	*ADSL*

29.3.3.2 Custom View for Ports Example

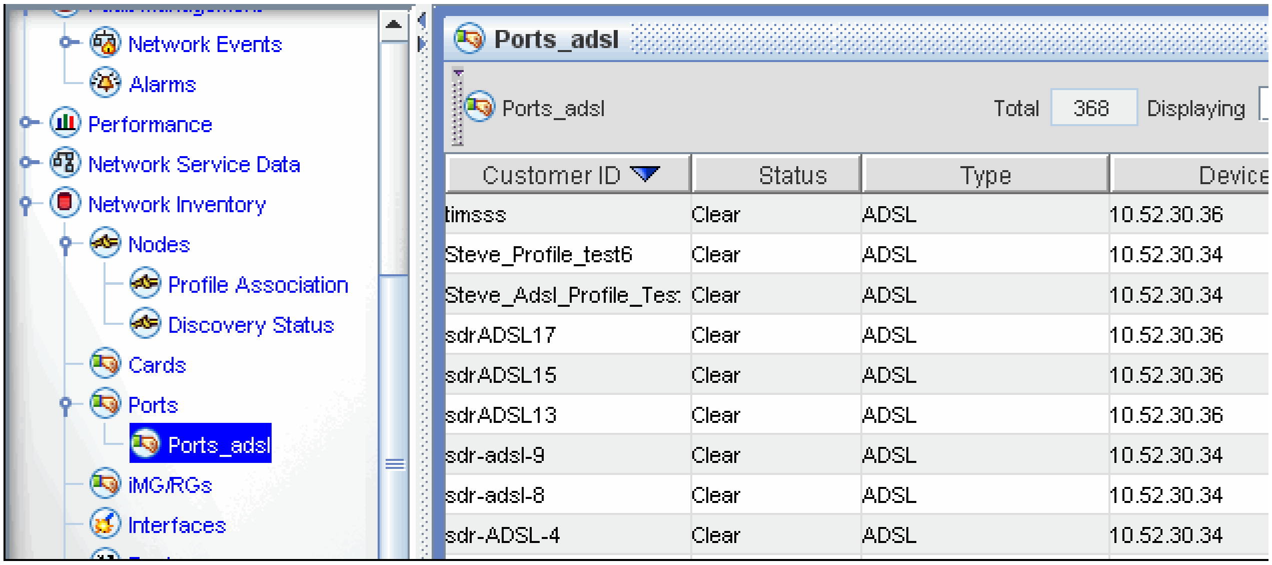
If there are a large number of ports being managed, the user can create a view that shows only ADSL ports. In the Custom View form, the user would:

1. Select **Ports** in the Inventory view and right-click *Custom View -> Add Custom View*.
2. In the **Filter View Name** field, type *Ports_adsl.*
3. Click **Next** to access the Additional Criteria, and type in *portType* and *adsl*, as follows.



Property Name	Match Criteria
☑ portType	adsl

4. Click on **OK**, and a Ports_adsl view is formed that shows only adsl ports, as follows.



Total 368 Displaying

Customer ID	Status	Type	Device
timsss	Clear	ADSL	10.52.30.36
Steve_Profile_test6	Clear	ADSL	10.52.30.34
Steve_Adsl_Profile_Tes	Clear	ADSL	10.52.30.34
sdrADSL17	Clear	ADSL	10.52.30.36
sdrADSL15	Clear	ADSL	10.52.30.36
sdrADSL13	Clear	ADSL	10.52.30.36
sdr-adsl-9	Clear	ADSL	10.52.30.34
sdr-adsl-8	Clear	ADSL	10.52.30.34
sdr-ADSL-4	Clear	ADSL	10.52.30.34

29.3.4 Interfaces (IP)

29.3.4.1 Properties

The following table lists the properties for interfaces. All the properties can be viewed by using the **Next** and **Back** button at the bottom of the form.

TABLE 29-7 Properties for Interfaces

MO Form Property	Description for Interfaces	Custom Map View Property (input this text)	Example
Name	The device name, which is a unique name that is used as the key in the database.	name	IF-172.16.33.11
DisplayName	The name by which the device is identified on the GUI.This is intended to be more intuitive regarding the identification of the device, whereas the name can be any string with the only constraint being that it is unique.	displayName	IF-172.16.33.11
Type	The type of the object, such as whether it is a network, node, or an interface object, or something user specified, like router, switch, network.	type	Always interface

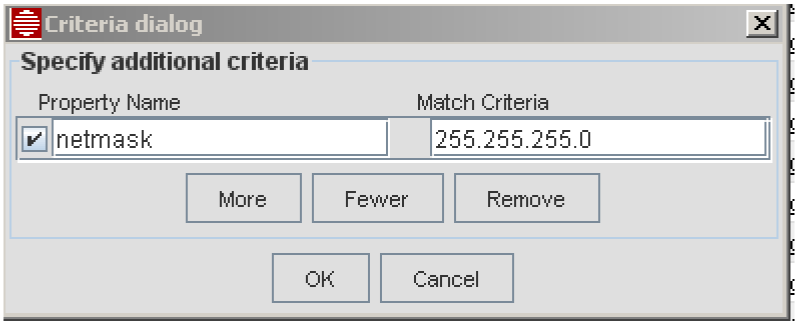
TABLE 29-7 Properties for Interfaces (Continued)

MO Form Property	Description for Interfaces	Custom Map View Property (input this text)	Example
IpAddress	The unique address assigned to each and every object.	ipAddress	172.16.33.11
Netmask	The netmask that is specified for this managed object. Network masking is a methodology by which the elements in a network can be meaningfully categorized.	netmask	255.255.255.128
ParentNet	The ID of the network that contains this interface.	parentNet	172.16.33.0
WriteCommunity	The SNMP community string for write access to agent used to reach this interface.	writeCommunity	private (for all SNMP communities for write access, all
SysOID	The system object identifier of the device as reported by the SNMP agent of the device.	sysOID	.1.3.6.1.4.1.207.1.15.3
ParentNode	The ID of the node on which the interface resides.	parentNode	172.16.33.11
Version	The version of the SNMP agent, such as v1, v2, or v3.	version	v2
IfDescr	The SNMP IfDescr value for this interface	ifDescr	MGMT:ETH:0
(More...)		stringstatus	Critical Major Minor Clear (separated by comma when choose more than one)
(More...)		hostNetmask	255.255.255.0

29.3.4.2 Custom View for Interfaces Example

The user can create a view that shows only interfaces for the 7700 devices. In the Custom View form, the user would:

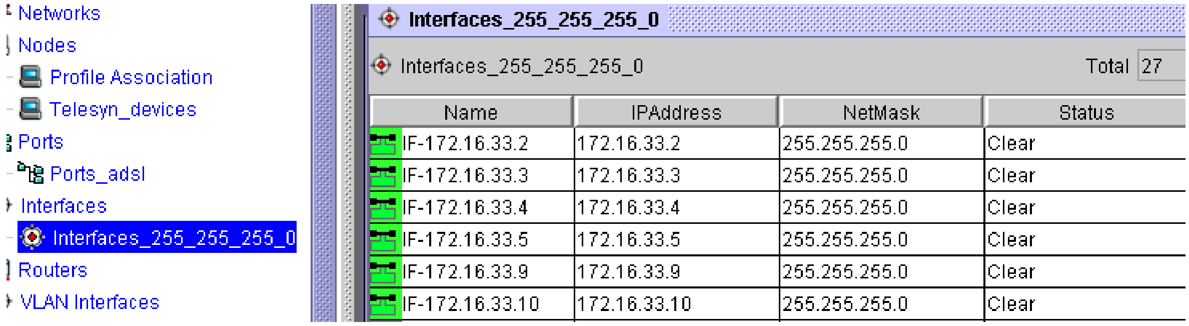
1. Select the Interfaces in the Inventory view and right-click *Custom View -> Add Custom View*.
2. In the **Filter View Name** field, type *Interfaces_255_255_255_0*.
3. Click **Next** to access the Additional Criteria, and type in *netmask* and *255.255.255.0*, as follows.



☑ netmask

255.255.255.0

4. Click on **OK**, and an Interfaces_255_255_255_0 view is formed that shows only interfaces with the 255.155.155.0 mask, as follows.



- Networks
- Nodes
  - Profile Association
  - Telesyn_devices
- Ports
  - Ports_adsl
- Interfaces
  - Interfaces_255_255_255_0
- Routers
- VLAN Interfaces

Interfaces_255_255_255_0

Interfaces_255_255_255_0 Total 27

Name	IPAddress	NetMask	Status
IF-172.16.33.2	172.16.33.2	255.255.255.0	Clear
IF-172.16.33.3	172.16.33.3	255.255.255.0	Clear
IF-172.16.33.4	172.16.33.4	255.255.255.0	Clear
IF-172.16.33.5	172.16.33.5	255.255.255.0	Clear
IF-172.16.33.9	172.16.33.9	255.255.255.0	Clear
IF-172.16.33.10	172.16.33.10	255.255.255.0	Clear

FIGURE 29-10 Interface Filter

29.3.5 Profiles

29.3.5.1 Properties

The following table lists the properties for profiles. All the properties can be viewed by using the **Next** and **Back** button at the bottom of the form.

TABLE 29-8 Managed Object Properties for Profiles

MO Form Property	Description for Profiles	Custom Map View Property (input this text)	Example
name	The name for each type of profile is a default and the name given by the user. Default names are: Profile_POTS Profile_Etherlike_Port Profile_ADSL Profile_Rapier_Device Profile_Telesyn_Device Profile_SwitchBlade_Device	name	Profile_POTS_test
type	type of object. This is always Profile.	type	Profile
(More...)		profileName	Test_Profile
(More...)		profileType	Profile

29.3.6 VLAN Interfaces

29.3.6.1 Properties

The following table lists the properties for VLAN interfaces. All the properties can be viewed by using the **Next** and **Back** button at the bottom of the form.

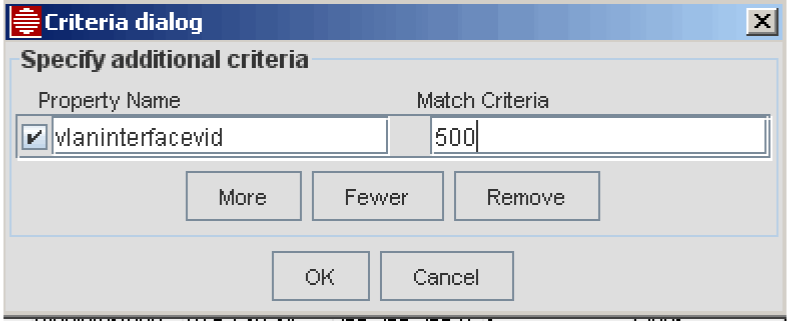
TABLE 29-9 Managed Object Properties for VLAN Interfaces

MO Form Property	Description for Interfaces	Custom Map View Property (input this text)	Example
DisplayName	The name by which the device is identified on the GUI.This is intended to be more intuitive regarding the identification of the device, whereas the name can be any string with the only constraint being that it is unique.	displayName	Default_VLAN
Name	The VIF name, which is a unique name that is used as the key in the database.	name	vlan999
pollInterval	The polling interval in seconds, which is the time gap between two successive status pollings of managed objects.	pollInterval	300
stringstatus	The status of the VLAN interface	stringstatus	Critical Major Minor Warning Clear Unknown (separated by comma when choose more than one)
type	The type of the object, such as whether it is a network, node, or an interface object, or something user specified, like router, switch, etc.	type	VlanInterface (Default)
vlanepsrtype		vlanepsrtype	Master Transit Data (All others)
vlangrouplist	The domain name for the vlan group, usually associated with an EPSR configuration	vlangrouplist	dom1,dom2
vlaninterfacevid	The VLAN ID associated with a Vlan interface. It is always set. The range: 1-4096.	vlaninterfacevid	500
vlantaggedports	A compact list of tagged ports on a VlanInterface. The list will be empty if none exist. The format is card.port delimited by commas.	vlantaggedports	11.1-9,12.1 - None (no ports are tagged)
Vlan Type	The type of VLAN (VLAN or HVLAN)	vlantype	VLAN HVLAN
UnTagged Ports	A compact list of untagged ports on a VLAN interface. The list will be empty if none exist.	vlanuntaggedports	11.1-9,12.1 - None (no ports are tagged)

29.3.6.2 Custom View for VLAN Interface Example

The user can create a view that shows only VLAN Interfaces for the VID 500. In the Custom View form, the user would:

1. Select the VLAN Interfaces in the Inventory view and right-click *Custom View -> Add Custom View*.
2. In the **Filter View Name** field, type VLAN_*500*.
3. Click Next to access the Additional Criteria, and type in *vlaninterfacevid* and *500*, as follows.

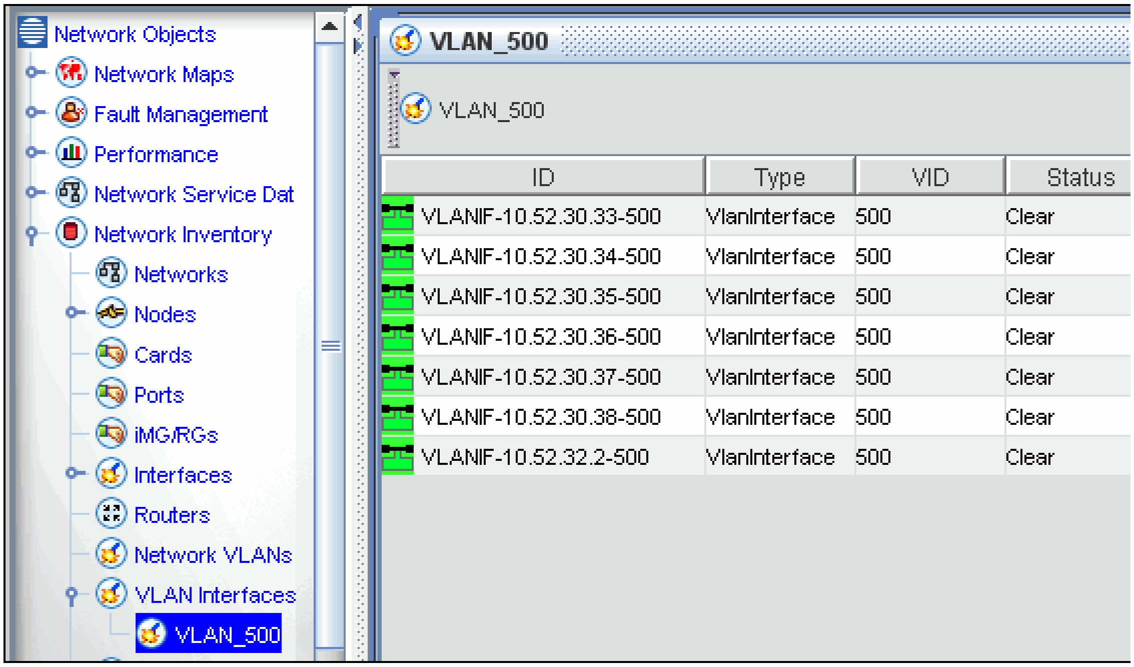


Criteria dialog

Specify additional criteria

Property Name	Match Criteria
☑ vlaninterfacevid	500

4. Click on **OK**, and a VLAN_500 view is formed that shows only interfaces with the 255.155.155.0 mask, as follows.



ID	Type	VID	Status
VLANIF-10.52.30.33-500	VlanInterface	500	Clear
VLANIF-10.52.30.34-500	VlanInterface	500	Clear
VLANIF-10.52.30.35-500	VlanInterface	500	Clear
VLANIF-10.52.30.36-500	VlanInterface	500	Clear
VLANIF-10.52.30.37-500	VlanInterface	500	Clear
VLANIF-10.52.30.38-500	VlanInterface	500	Clear
VLANIF-10.52.32.2-500	VlanInterface	500	Clear

FIGURE 29-11 VLAN Filter

29.3.7 Physical Links

29.3.7.1 Properties

The following table lists the properties for physical links. All the properties can be viewed by using the **Next** and **Back** button at the bottom of the form.

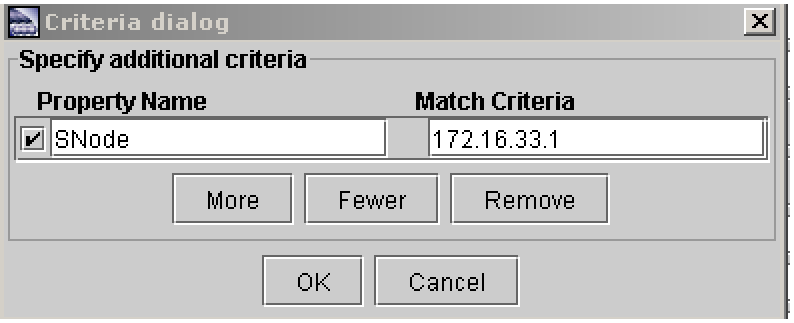
TABLE 29-10 Managed Object Properties for Physical Links

MO Form Property	Description for Interfaces	Custom Map View Property (input this text)	Example
Name	The device name, which is a unique name that is used as the key in the database.	name	LINK-172.16.33.14-9--172.16.33.10-5 (This follows the format of device-link--device-link)
Link Type	The type of the object, such as whether it is a network, node, or an interface object, or something user specified, like router, switch, etc.	type	L2LinkMO
SNode	The source node of a physical link.	SNode	17.16.33.10
Destination port	The destination port of a physical link.	DPort	1.1
Dest. Device	The destination device of a physical link.	DNode	2.1
Source port	The source port of a physical link.	SPort	1.1
(More...)		stringstatus	Critical Major Minor Warning Clear (separated by comma when choose more than one)

29.3.7.2 Custom View for Physical Links Example

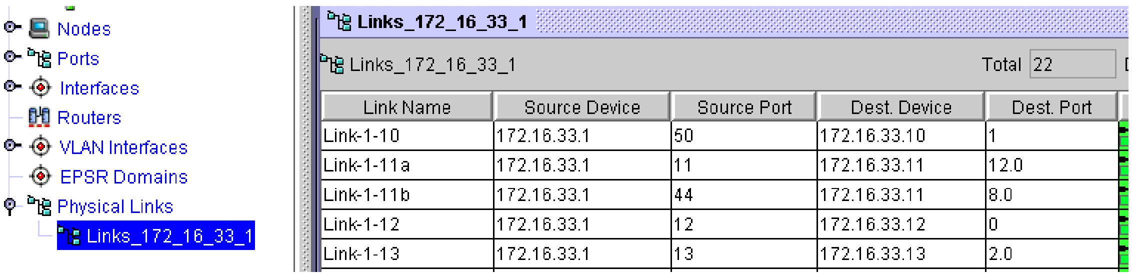
The user can create a view that shows only VLAN Interfaces for the VID 500. In the Custom View form, the user would:

1. Select the VLAN Interfaces in the Inventory view and right-click *Custom View -> Add Custom View*.
2. In the name field, type Links_172_16_33_1.
3. Click Next to access the Additional Criteria, and type in SNode and 172.16.33.1, as follows.



☑ SNode 172.16.33.1

4. Click on **OK**, and a Links_172_16_33_1 view is formed that shows only interfaces with the 255.155.155.0 mask, as follows.



Links_172_16_33_1

Links_172_16_33_1 Total 22

Link Name	Source Device	Source Port	Dest. Device	Dest. Port
Link-1-10	172.16.33.1	50	172.16.33.10	1
Link-1-11a	172.16.33.1	11	172.16.33.11	12.0
Link-1-11b	172.16.33.1	44	172.16.33.11	8.0
Link-1-12	172.16.33.1	12	172.16.33.12	0
Link-1-13	172.16.33.1	13	172.16.33.13	2.0

FIGURE 29-12 Mask Filter

29.3.8 Performance Monitoring

29.3.8.1 Properties

A complete list of the object properties for a polling object is in the AlliedView NMS Administration Guide. The following table lists the properties that are used when creating a custom map view.

TABLE 29-11 Properties for Statistics

MO Form Property	Description	Custom Map View Property (input this text)	Example
Name	Any meaningful string for the Data Identifier.	name	etherStatsPkts
SnmpVersion	One of the three SNMP versions - V1, V2 or V3. **Required**.	snmpVersion	v2
Read Community	Enter the string with which the devices are identified in a network. Most of the equipment vendors set the Community value as **public** for their devices, so it is usually used here. Otherwise you have to check the string used for the particular device. *Note: The community specified must be enabled on the device.*	community	public
OID	A unique Object Identifier string that represents a MIB entry. Data is collected for this identifier. An SNMP specific Data identifier is called an **OID**. For example, 2.2.1.16.1 refers to IfInOctects interface instance 1. **Required**.	oid	.1.3.6.1.2.1.16.1.1.1.5
Agent	Normally a device will have one agent in it to collect device data, and the device name and agent name will be the same. **Required**.	agent	172.16.33.11
DNS Name	Name of the device from which data have to be collected.	dnsName	172.16.33.11
Active	A checkbox, when checked, means the data collection will be started for this OID. (The statistic row once created will be green.) Default value: False (unchecked).	active	false

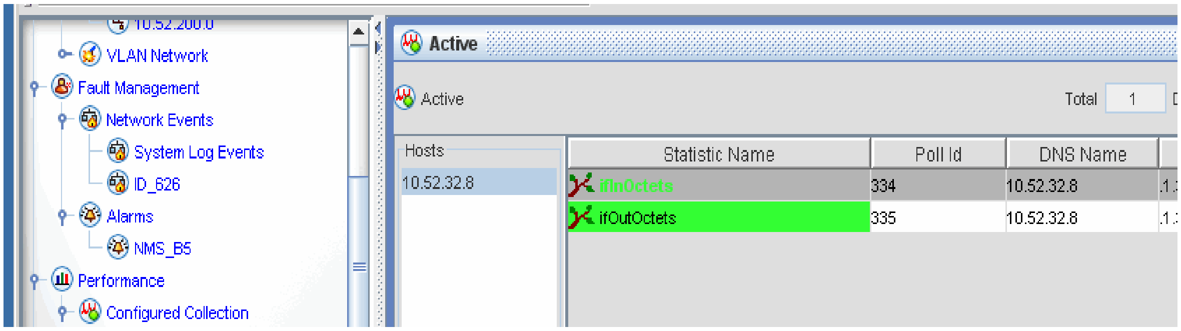
TABLE 29-11 Properties for Statistics

MO Form Property	Description	Custom Map View Property (input this text)	Example
Period	The time interval for periodic data collection. For example, if set to 2, for all the Data identifiers, data will be collected once in every 2 seconds. Default value: 300 seconds.	period	300 (the default value)
Threshold	Checking means the Threshold will be applied on this Data identifier. Unchecked means no Threshold will be applied. Default value: False (unchecked).	threshold	false
failureThreshold	Threshold at which a failure is declared.	failureThreshold	1
Multiple	Checking means the data identifier is of type multiple.	isMultiplePolledData	true
saveAbsolutes	This option is applicable only for Counter type OIDs. By default, data collected for Counter type OIDs is not stored as it is. The difference between the previous data and latest data is collected and stored. If the exact value (absolute value) of collected data has to be stored for Counter type OIDs, then this check box should be checked. Data collected for OIDs of other data types are saved as absolute values. Default value: False (Unchecked).	saveAbsolutes	false
SaveOn Threshold	Possible values are true and false. If true the collected data is saved only when it exceeds the threshold. Default value: false	saveOnThreshold	false
Time Average	Checking means the Time Average will be calculated as follows: (<Latest collected value> + <Previous collected value>) / <Difference in data collection Time value> This is mostly calculated for counter type and gauge type OIDs where the data collected will be an incremental value and at one point will reach the final value and reset to zero. As this reset may happen soon and very often, it is preferred that a delta value is derived from two consecutive polls. Default value: false.	timeAvg	false
Last Counter Value	The counter value last read.	lastCounterValue	0
Last Time Value	The time the counter was last read.	lastTimeValue	0
Log Directly	Checking means to store the collected data in flat files rather than storing them in database. Default value: false (unchecked).	log Directly	false
Poll ID	A unique number associated with each Statistic to identify the Statistic. Poll ID is automatically generated so no two Statistics will have the same Poll ID.	id	334

29.3.8.2 Custom View for Statistics Example

The user can create a view that shows which statistics match a DNS Name. In the Custom View form, the user would:

1. Select the Configured Collection in the Performance view and right-click *Custom View -> Add Custom View*.
2. In the Filter View Name, type *Active*.
3. In the Active pulldown, select *True*.
4. Click on **OK**, and a view is formed that shows only devices with activated statistics, as follows. (Click on each device to see the active statistics.)



Total 1

Hosts
10.52.32.8

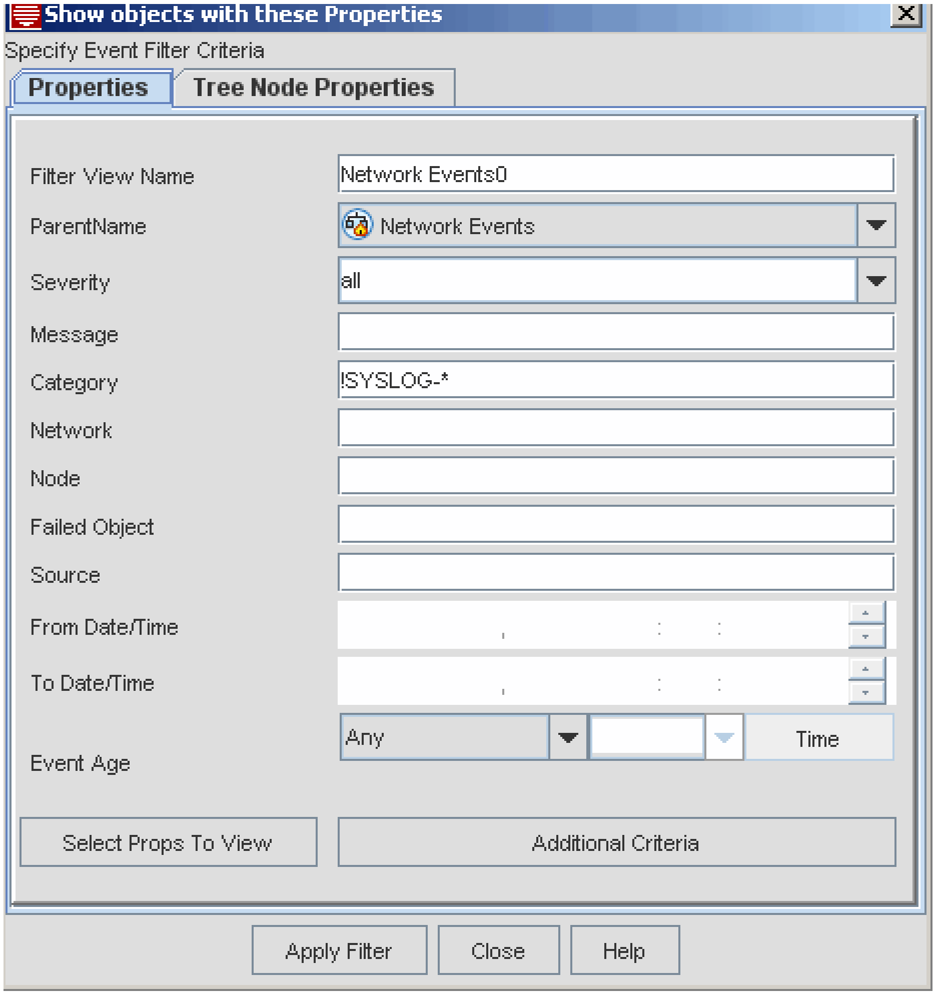
Statistic Name	Poll Id	DNS Name	
ifInOctets	334	10.52.32.8	.1
ifOutOctets	335	10.52.32.8	.1

FIGURE 29-13 Statistics Filter

29.3.9 Events

29.3.9.1 Properties

You can set the match criteria by using the Specify Event Filter Criteria form. This form can be accessed by selecting *Custom Views -> Add Custom Views* from the Panel-Specific Menu Bar. Refer to the following figure.



Show objects with these Properties

Specify Event Filter Criteria

Filter View Name	Network Events0
ParentName	Network Events
Severity	all
Message	
Category	!SYSLOG-*
Network	
Node	
Failed Object	
Source	
From Date/Time	
To Date/Time	
Event Age	Any

FIGURE 29-14 Matching Properties Form for Events

The following table lists the properties in detail.

TABLE 29-12 Custom View Criteria for Events

MO Form Property	Description for Match Properties	Custom View Property Name (input this text)	Example
Severity	The severity of the object. Severity is a property in the event object that indicates the criticality of the event. The severity of the event to be filtered can be assigned using the combo box. Multiple severities can also be assigned by separating them using a comma.	severity	Major (if multiple, separate with commas)
Category	A value that can help in useful categorization of the alarm. Note that the default is !SYSLOG-*, since the SYSLOG events are listed in the System Log Events leaf node.	category	Port (Port has been affected)

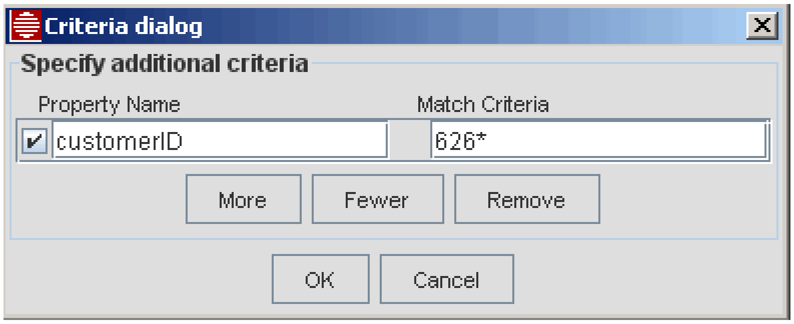
TABLE 29-12 Custom View Criteria for Events

MO Form Property	Description for Match Properties	Custom View Property Name (input this text)	Example
Failed Object	Information about the specific entity within the source of the event, which is primarily responsible for the occurrence of this alarm. The name of the failure object to be filtered can be given in this field.	entity	ADSL_172.16.33.19;adslAtucUASL_Port0.15 (Separated with semicolons, these are objects affected by the alarm)
customerID	The Customer ID assigned when provisioning for triple-play	customerID	746*

29.3.9.2 Custom View for Events Example

The user can create a view that shows which events are associated with a specific subscriber. In the Custom View form, the user would:

1. Select the Network Events in the Fault Managements view and right-click *Custom View -> Add Custom View*.
2. In the name field, type *ID_626*.
3. Click Next to access the Additional Criteria, and type in *626**, as follows.

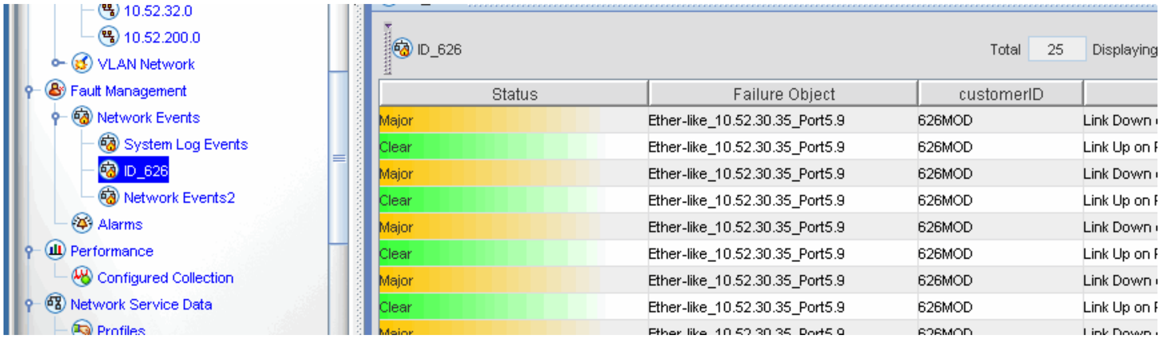


Criteria dialog

Specify additional criteria

Property Name	Match Criteria
☑ customerID	626*

4. Click on **OK**, and a view is formed that shows only events associated with customer IDs that include 626, as follows. (Click on each event for details.)



ID_626 Total 25 Displaying

Status	Failure Object	customerID	
Major	Ether-like_10.52.30.35_Port5.9	626MOD	Link Down
Clear	Ether-like_10.52.30.35_Port5.9	626MOD	Link Up on
Major	Ether-like_10.52.30.35_Port5.9	626MOD	Link Down
Clear	Ether-like_10.52.30.35_Port5.9	626MOD	Link Up on
Major	Ether-like_10.52.30.35_Port5.9	626MOD	Link Down
Clear	Ether-like_10.52.30.35_Port5.9	626MOD	Link Up on
Major	Ether-like_10.52.30.35_Port5.9	626MOD	Link Down
Clear	Ether-like_10.52.30.35_Port5.9	626MOD	Link Up on
Major	Ether-like_10.52.30.35_Port5.9	626MOD	Link Down

FIGURE 29-15 Customer ID Filter

29.3.10 Alarms

29.3.10.1 Properties

The following table lists the properties for Alarms and the ones used for setting up criteria for custom alarm views.

TABLE 29-13 Properties for Alarm Criteria

MO Form Property	Description for Criteria - Alarms	Property for Custom View (input this text)	Example
Severity	The level of the alarm. The severity of the alarm to be filtered can be assigned using the combo box. Multiple severities can also be assigned by separating them using a comma.	severity	Critical Major Minor Warning Clear (separated by comma when choose more than one)
Previous severity	The match criteria based on the previous severity of the alarm.	previousSeverity	Critical Major Minor Warning Clear (separated by comma when choose more than one
Owner	The name of the owner of the alarm.	owner	Paul
Category	The category for the alarm.	category	Telesyn (for MAP devices)
Message	Any additional information. To use, fill the message in and alarms with the corresponding message are displayed.	message	Unavailable seconds-line 15-minute threshold
Failure object	Information about the specific entity, within the source of the alarm, which is primarily responsible for the alarm. When filled in, it provides a filter.	entity	ADSL_172.16.33.19;adslAtucUASL_Port0.15 (Separated with semicolons, these are objects affected by the alarm)
Source	Information about the source of the alarm. When filled in, it provides a filter.	source	172.16.33.19
From Date/Time (modified)	The date and time after which alarms that are modified are displayed. Format is month, date, year, hour, minute, second and AM / PM	Form has GUI	
To Date/Time (modified)	The date and time before which alarms that are modified are displayed. Format is month, date, year, hour, minute, second and AM / PM	Form has GUI	
From Date/Time (Created)	The date and time after which alarms that are generated are displayed. Format is month, date, year, hour, minute, second and AM / PM	Form has GUI	

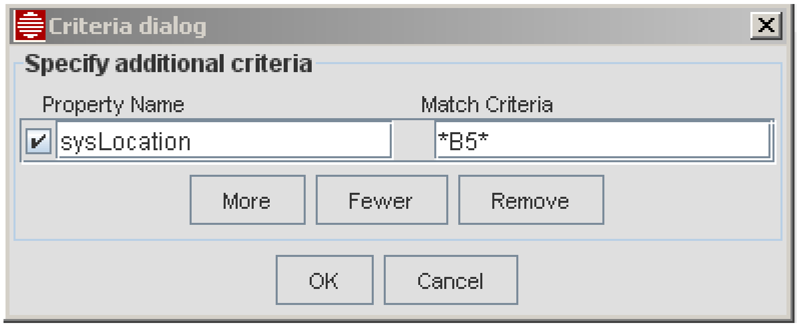
TABLE 29-13 Properties for Alarm Criteria (Continued)

MO Form Property	Description for Criteria - Alarms	Property for Custom View (input this text)	Example
To Date/Time (created)	The date and time before which alarms that are generated are displayed. Format is month, date, year, hour, minute, second and AM / PM	Form has GUI	
Alarm Age (modified time)	The age of the alarm for filtering purposes. The age of an alarm is the time lapsed since the last modification of the alarm in the NMS system. The alarm age property can be age in min, age in hrs, age in days, today, yesterday and so on.	Form has GUI	
id	The id number given to the alarm	id	41931
(More...)		notes	Unavailable seconds-line 15-minute threshold
(More...)		priority	0
(More...)		sysLocation	see "Example of Custom Alarm Filter (Alarms by Location)" on page 1081.

29.3.10.2 Example of Custom Alarm Filter (Alarms by Location)

In this example, custom alarm views are created in which each view contains alarms from a specific location.

1. In the Object tree, select the Alarms node icon and right click *Custom Views* -> *Add Custom Views* (selecting the Alarms node is not necessary, but helps set the location of the custom view, as shown below).
2. In the **Specify Alarm Filter Criteria** window, change the name of the view to *NMS_B5*.
3. Click on Additional Criteria, then input the Property Name and match criteria. The property name we are using is sysLocation, and the criteria we are using is the string *Raleigh*, which we configured when providing device information. Figure 29-16 shows the example.



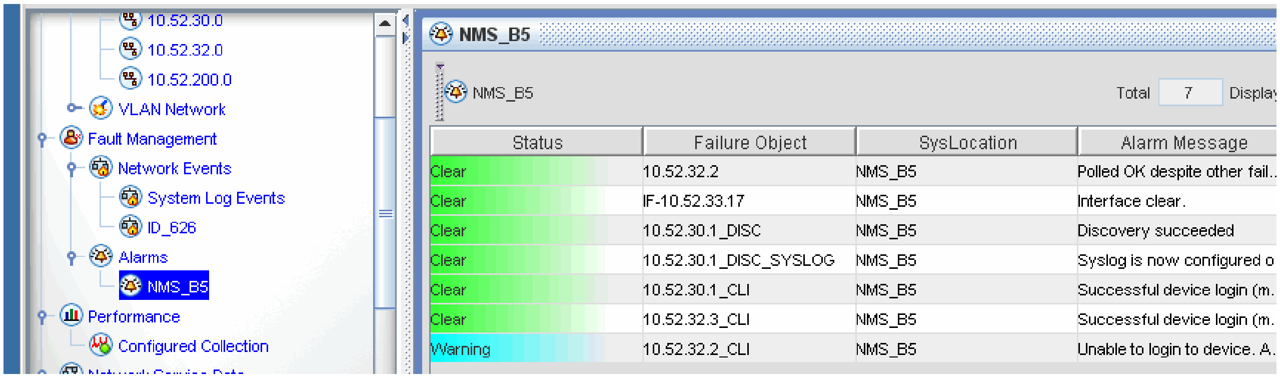
Criteria dialog

Specify additional criteria

Property Name	Match Criteria
☑ sysLocation	*B5*

FIGURE 29-16 Setting Criteria for Custom Alarm View (sysLocation)

4. Select the tic box, OK, and then **Apply Filter**. Now when the NMS_B5 custom view is shown, only those devices with the sysLocation of B5 are listed in the view, as shown in Figure 29-17.



Status	Failure Object	SysLocation	Alarm Message
Clear	10.52.32.2	NMS_B5	Polled OK despite other fail..
Clear	IF-10.52.33.17	NMS_B5	Interface clear.
Clear	10.52.30.1_DISC	NMS_B5	Discovery succeeded
Clear	10.52.30.1_DISC_SYSLOG	NMS_B5	Syslog is now configured o
Clear	10.52.30.1_CLI	NMS_B5	Successful device login (m.
Clear	10.52.32.3_CLI	NMS_B5	Successful device login (m.
Warning	10.52.32.2_CLI	NMS_B5	Unable to login to device. A.

FIGURE 29-17 Example of Showing Alarms for Specific Location

29.4 Custom Physical Maps with Links

Links can be added to the custom Physical Maps. However, certain criteria must be used to create a custom map that will allow link symbols to be placed on it. These are described below.

29.4.1 Adding Links to Existing Custom Physical Map

To add links to an existing map (provided it's criteria are suitable) refer to the following figure, which shows the system Physical Map and links between 9000-type devices.

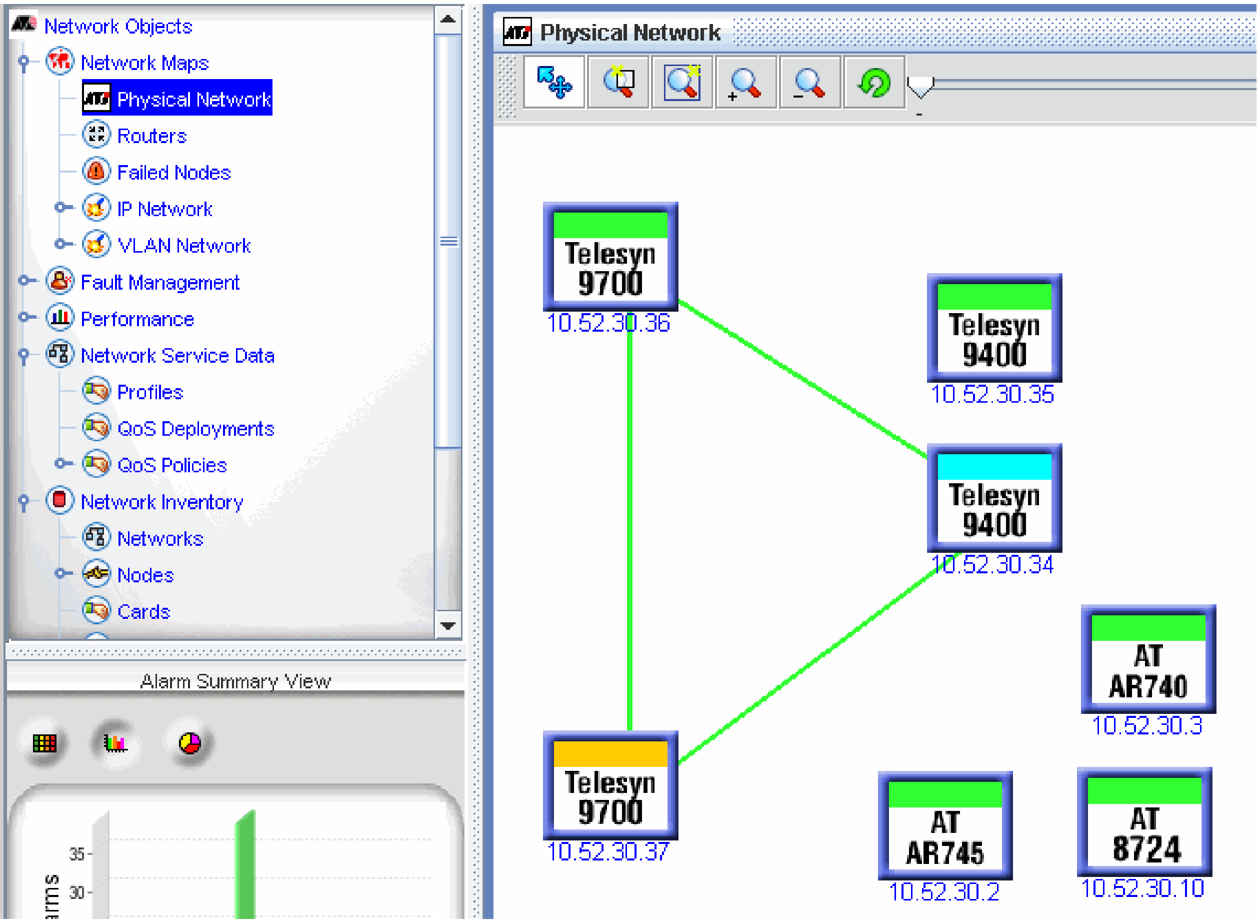


FIGURE 29-18 Physical Map with Links

For links to be added to a custom map, the map's criteria can only include the following parameters:

- "name"
- "classname"
- "type"

Use one or more of these parameters to specify a set of iMAP devices, then the *Add Links To Map* operation will automatically create link lines for the Links that are defined in the NMS and have end ports on iMAPs existing on the custom map.

For example, if you are using DNS names and they are assigned so that the initial/final characters of each device's name identifies the custom map that you would like it to be on, then a "name" criteria could be used to collect those devices onto a single Custom Map. Specifically, if the devices RAL1, RAL2, …, RAL30 are to be put on a single Custom Map, then use the criteria "name=RAL*" for that map.

If not using DNS, then the names will look like IP addresses, and a subnet map can be matched by a pattern like "name=172.16.33.*".

You can also use "type" to separate-off by device type (e.g., 9700, 9400, 9*, …).

The classname should be CLISNMPNodeMO to pick up iMAP devices only; otherwise many Port objects can appear on the custom map.

To create a custom map that looks like the Physical Map and also has links, do the following:

1. *Custom Views-> Add New Map*
2. Set topology to "grid(isActualIconSize=true;gapX=20;gapY=20;cellWidth=100;cellHeight=100;scroll=vertical),star,ring,flow"
3. Set mapSymbolRenderer="com.adventnet.nms.mapui.ATIMapSymbolRendererImpl_3"
4. Add criteria by selecting "more" at the bottom of the window.
   - Only use the following criteria names if Links are to be added later:

     - name (e.g. name = 172.16.33.*)

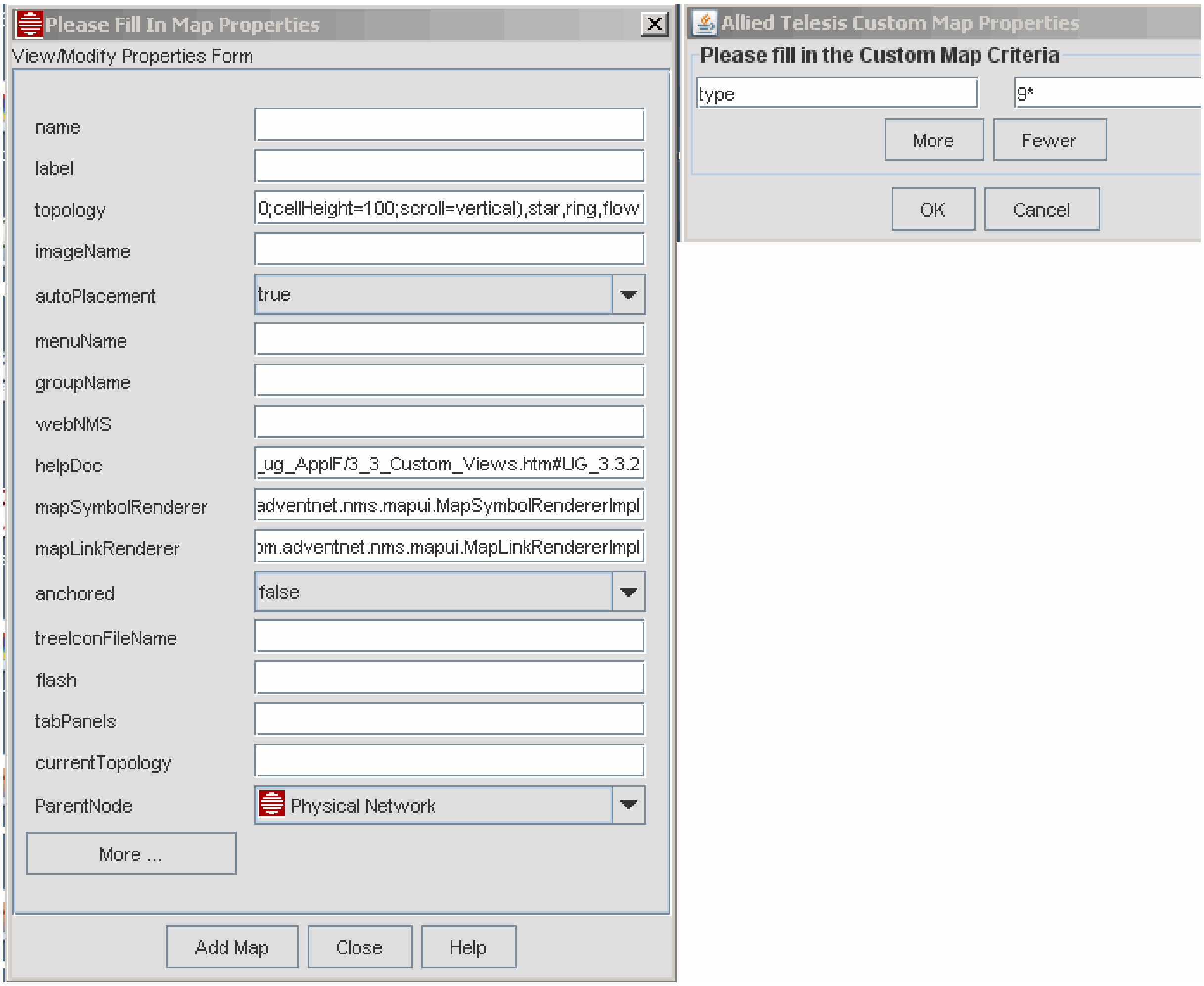
     - classname (e.g. classname = CLISNMPNodeMO)

     - type (e.g. type = 9700)

Note: These can be updated to also include linksets, which is what the Add Links operation will do.

   - The map will be created looking like the Physical Map but the background is gray (instead of white) and no links will show. (To update the background, double-click the background and in the Map Properties tab add an ImageName.)
5. While the custom map is active, select the *View -> Add Links to Map* and the map will now have link lines drawn.
6. Refer to the following figures.

Note: The system Physical Map and custom Physical Map have the same features and interact; When new links are created or old links deleted on the system Physical Map they will now be automatically updated on the Custom map, and vise versa.



Please Fill In Map Properties

View/Modify Properties Form

name	
label	
topology	0;cellHeight=100;scroll=vertical),star,ring,flow
imageName	
autoPlacement	true
menuName	
groupName	
webNMS	
helpDoc	_ug_ApplF/3_3_Custom_Views.htm#UG_3.3.2
mapSymbolRenderer	adventnet.nms.mapui.MapSymbolRendererImpl
mapLinkRenderer	om.adventnet.nms.mapui.MapLinkRendererImpl
anchored	false
treeIconFileName	
flash	
tabPanels	
currentTopology	
ParentNode	Physical Network

Allied Telesis Custom Map Properties

Please fill in the Custom Map Criteria

type	9*

FIGURE 29-19 Setting Custom Physical Map Criteria

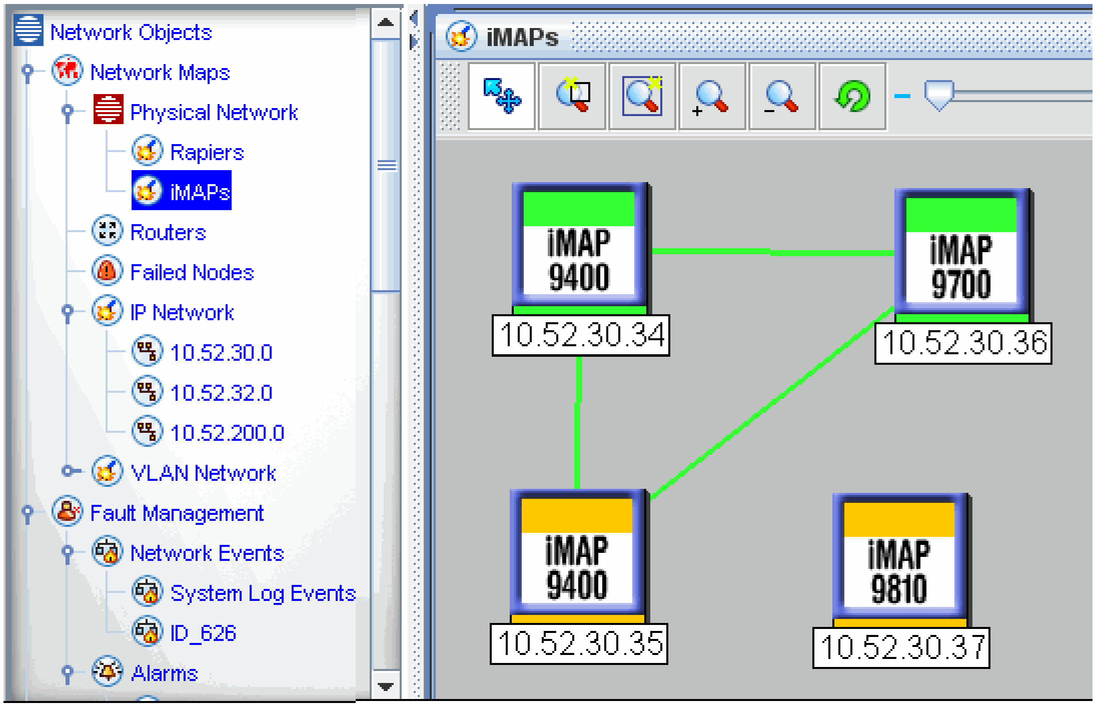


FIGURE 29-20 Adding the Links to the Custom Physical Map

30. Exporting Tabular Data

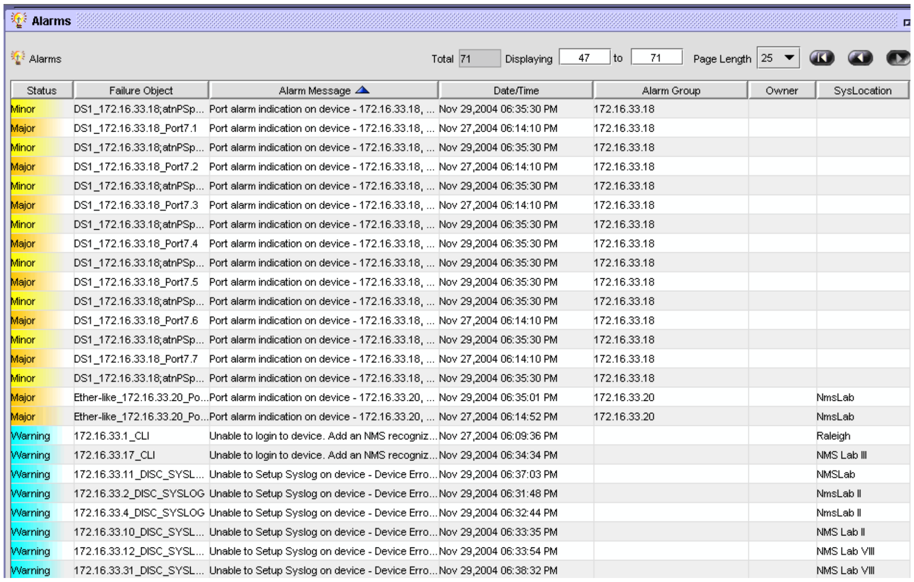
Data displayed in tabular form in the AlliedView NMS can be exported to a file on the NMS server or to your Web browser for viewing. Tabular data appears in the following views:

- Fault Management
- Performance
- Network Inventory

The procedure for exporting tabular data is the same for all of these views.

Note: The one exception is the Performance view; this is explained separately, in "Exporting Performance Data" on page 1089.

To demonstrate the procedure, the data in the Alarms subview will be exported in this section. The Alarms subview is shown in the following figure.



Total 71 Displaying 47 to 71 Page Length 25

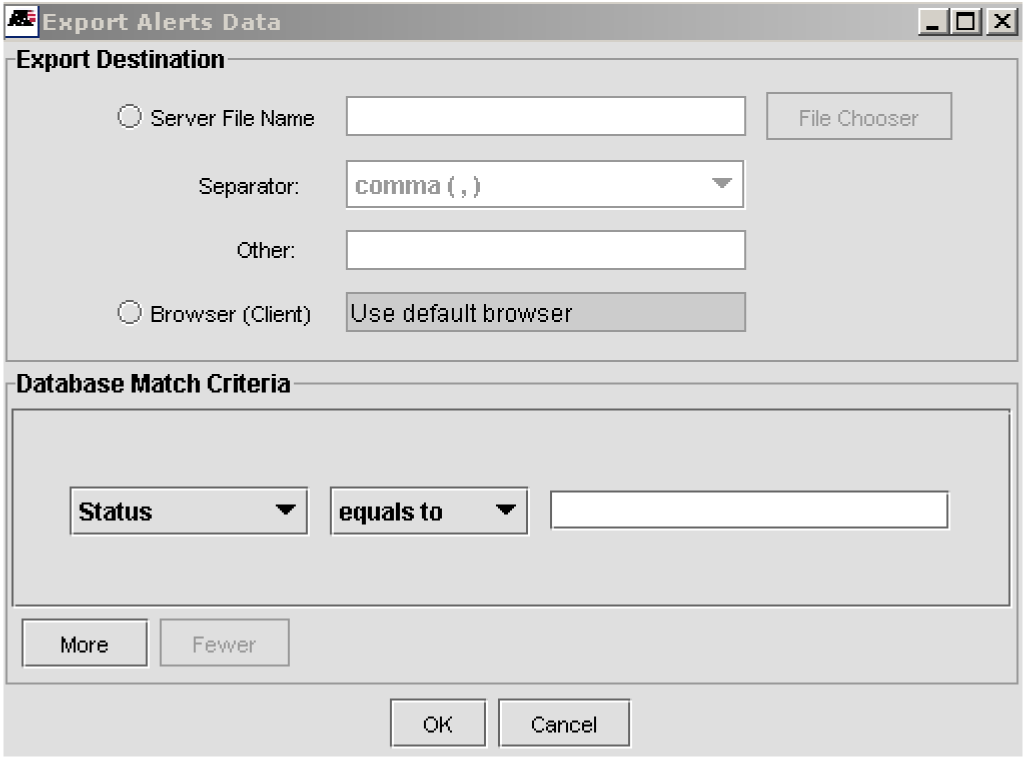
Status	Failure Object	Alarm Message	Date/Time	Alarm Group	Owner	SysLocation
Minor	DS1_172.16.33.18;atnPSp...	Port alarm indication on device - 172.16.33.18, ...	Nov 29,2004 06:35:30 PM	172.16.33.18		
Major	DS1_172.16.33.18_Port7.1	Port alarm indication on device - 172.16.33.18, ...	Nov 27,2004 06:14:10 PM	172.16.33.18		
Minor	DS1_172.16.33.18;atnPSp...	Port alarm indication on device - 172.16.33.18, ...	Nov 29,2004 06:35:30 PM	172.16.33.18		
Major	DS1_172.16.33.18_Port7.2	Port alarm indication on device - 172.16.33.18, ...	Nov 27,2004 06:14:10 PM	172.16.33.18		
Minor	DS1_172.16.33.18;atnPSp...	Port alarm indication on device - 172.16.33.18, ...	Nov 29,2004 06:35:30 PM	172.16.33.18		
Major	DS1_172.16.33.18_Port7.3	Port alarm indication on device - 172.16.33.18, ...	Nov 27,2004 06:14:10 PM	172.16.33.18		
Minor	DS1_172.16.33.18;atnPSp...	Port alarm indication on device - 172.16.33.18, ...	Nov 29,2004 06:35:30 PM	172.16.33.18		
Major	DS1_172.16.33.18_Port7.4	Port alarm indication on device - 172.16.33.18, ...	Nov 29,2004 06:35:30 PM	172.16.33.18		
Minor	DS1_172.16.33.18;atnPSp...	Port alarm indication on device - 172.16.33.18, ...	Nov 29,2004 06:35:30 PM	172.16.33.18		
Major	DS1_172.16.33.18_Port7.5	Port alarm indication on device - 172.16.33.18, ...	Nov 29,2004 06:35:30 PM	172.16.33.18		
Minor	DS1_172.16.33.18;atnPSp...	Port alarm indication on device - 172.16.33.18, ...	Nov 29,2004 06:35:30 PM	172.16.33.18		
Major	DS1_172.16.33.18_Port7.6	Port alarm indication on device - 172.16.33.18, ...	Nov 27,2004 06:14:10 PM	172.16.33.18		
Minor	DS1_172.16.33.18;atnPSp...	Port alarm indication on device - 172.16.33.18, ...	Nov 29,2004 06:35:30 PM	172.16.33.18		
Major	DS1_172.16.33.18_Port7.7	Port alarm indication on device - 172.16.33.18, ...	Nov 27,2004 06:14:10 PM	172.16.33.18		
Minor	DS1_172.16.33.18;atnPSp...	Port alarm indication on device - 172.16.33.18, ...	Nov 29,2004 06:35:30 PM	172.16.33.18		
Major	Ether-like_172.16.33.20_Po...	Port alarm indication on device - 172.16.33.20, ...	Nov 29,2004 06:35:01 PM	172.16.33.20		NmsLab
Major	Ether-like_172.16.33.20_Po...	Port alarm indication on device - 172.16.33.20, ...	Nov 27,2004 06:14:52 PM	172.16.33.20		NmsLab
Warning	172.16.33.1_CLI	Unable to login to device. Add an NMS recogniz...	Nov 27,2004 06:09:36 PM			Raleigh
Warning	172.16.33.17_CLI	Unable to login to device. Add an NMS recogniz...	Nov 29,2004 06:34:34 PM			NMS Lab III
Warning	172.16.33.11_DISC_SYSL...	Unable to Setup Syslog on device - Device Erro...	Nov 29,2004 06:37:03 PM			NMSLab
Warning	172.16.33.2_DISC_SYSLOG	Unable to Setup Syslog on device - Device Erro...	Nov 29,2004 06:31:48 PM			NmsLab II
Warning	172.16.33.4_DISC_SYSLOG	Unable to Setup Syslog on device - Device Erro...	Nov 29,2004 06:32:44 PM			NmsLab II
Warning	172.16.33.10_DISC_SYSL...	Unable to Setup Syslog on device - Device Erro...	Nov 29,2004 06:33:35 PM			NMS Lab II
Warning	172.16.33.12_DISC_SYSL...	Unable to Setup Syslog on device - Device Erro...	Nov 29,2004 06:33:54 PM			NMS Lab VIII
Warning	172.16.33.31_DISC_SYSL...	Unable to Setup Syslog on device - Device Erro...	Nov 29,2004 06:38:32 PM			NMS Lab VIII

FIGURE 30-1 Alarms Subview

The entire table can be exported to a file or only selected items in the list.

30.1 Exporting Subviews

To export the entire table, select *Edit -> Export Table Data* from the Panel-Specific Menu Bar. The Export PhysicalLinks Data form, shown in the following figure, will appear.



○ Server File Name

Separator: comma (,)

Other:

○ Browser (Client) Use default browser

Status equals to

FIGURE 30-2 Export Alarms Data Form - No Criteria Set

The Export Alarms Data from consists of a destination panel and a database match criteria panel. In the destination panel, you can select the destination for the exported data as either a file on the NMS server or your Web browser. In the Database Match Criteria panel, you can specify the match criteria, a qualifier, and a match string. The criteria correspond to fields in the data table, such as **Status**, **Owner. Alarm Message**, etc. The qualifiers are match specifications, such as equals to, not equals to, contains, etc. The match string field is where you type the string you want to match.

The radio buttons in the **Export Destination** panel allow you to specify the data destination. To send the data to your Web browser, click the **Browser (Client)** radio button. If you have more than one Web browser on your machine, select the desired browser.

To send the data to a file, do the following:

1. Click the **Text File (Server)** radio button
2. Click **File Chooser**. The **Open** form will appear.
3. In the **Open** form, double-click **state** in the directory view panel.

Note: *You must store your file in the state directory. If you attempt to store your file in any other directory, you will get an error message.*

4. Type the desired filename in the **File Name** field, and then click **Open**. The **Open** form will close, and the file you chose will appear in the **Text File (Server)** field of the **Export Alerts Data** form.
5. Select a data separator from the **Separator** drop-down list. If the desired separator is not in the list, select **other (specify)**, and then type the desired separator in the **Other** field.

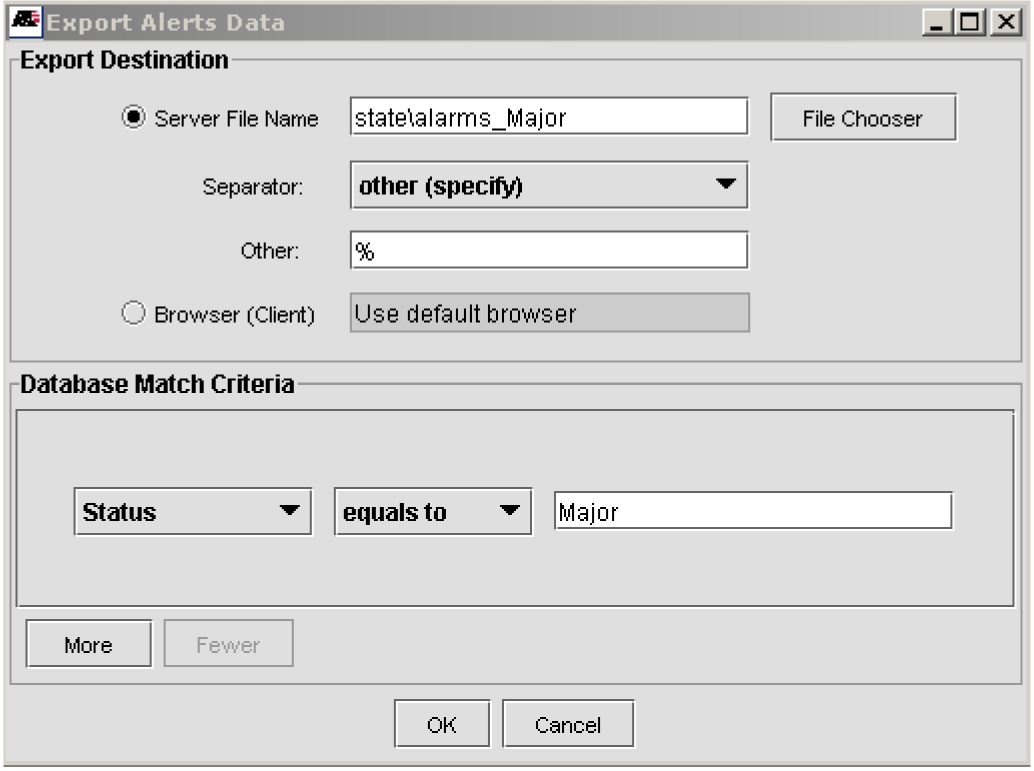
Once you have specified the data destination, specify the match criteria in the **Database Match Criteria** panel as follows:

1. Select a criteria from the drop-down list, select a qualifier from the qualifier drop-down list, and then enter a match string in the match string field.
2. If you need more qualifiers, click **More,** and then enter the additional qualifier. Repeat as necessary.

Note: Click Fewer to remove the last qualifier that you added.

3. Click **OK** to export the data. A confirmation dialog box will appear indicating that the data export was successful. Click **OK** in the confirmation dialog box.

The following figure shows an example of how to export all major alarms on device to file **alarms_major** using the percent sign (%) as the data separator. The resulting data file is described in "Viewing a Data Export File" on page 1092.



Export Alerts Data

Export Destination

● Server File Name: state\alarms_Major

Separator: other (specify)

Other: %

○ Browser (Client): Use default browser

Database Match Criteria

Status | equals to | Major

FIGURE 30-3 Export Major Alarms Data Example

30.2 Exporting Performance Data

Performance Data is different in that each statistic is counted against what is called an instance, or component. The following figure shows these instances when plotting a statistic for a device. The pull-down shows that the VLAN number IDs as well as the port numbers are instances statistics can be counted against.

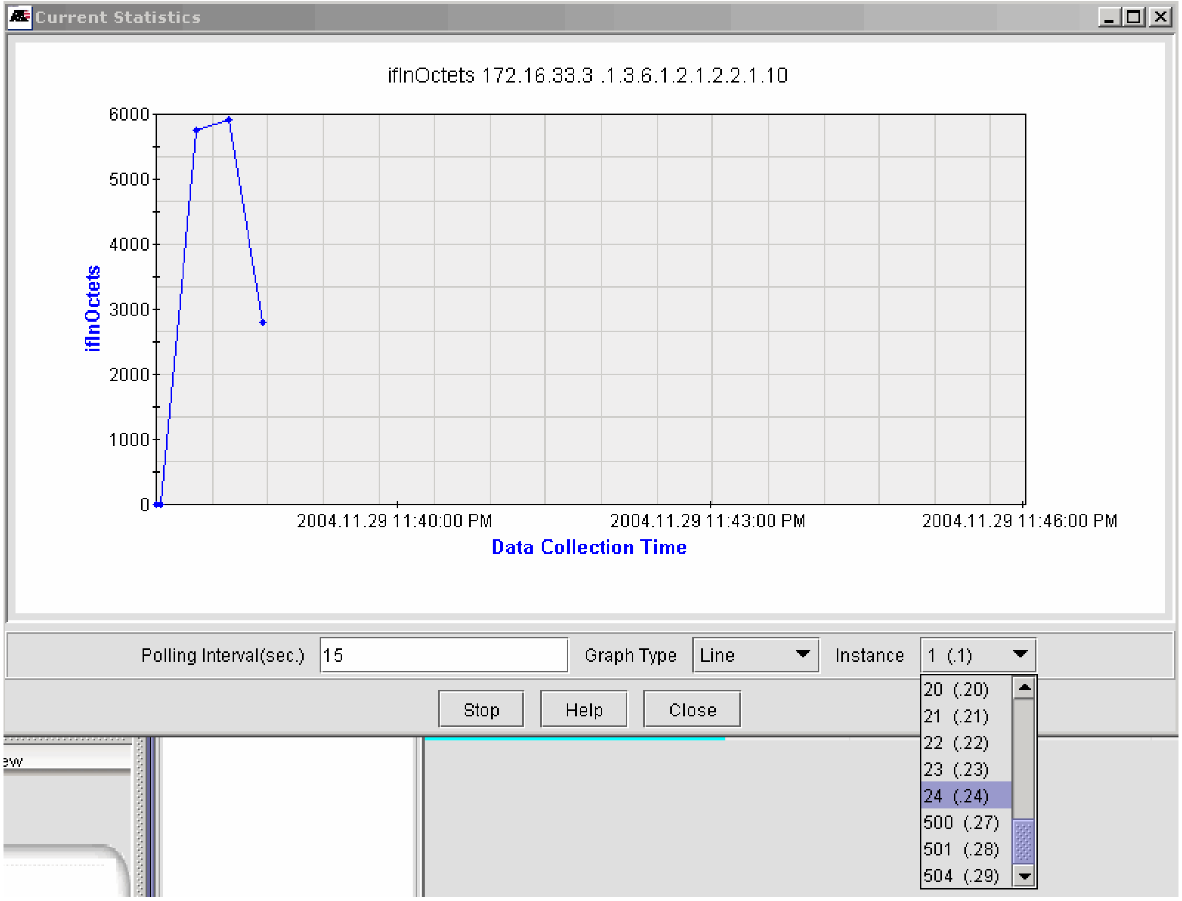
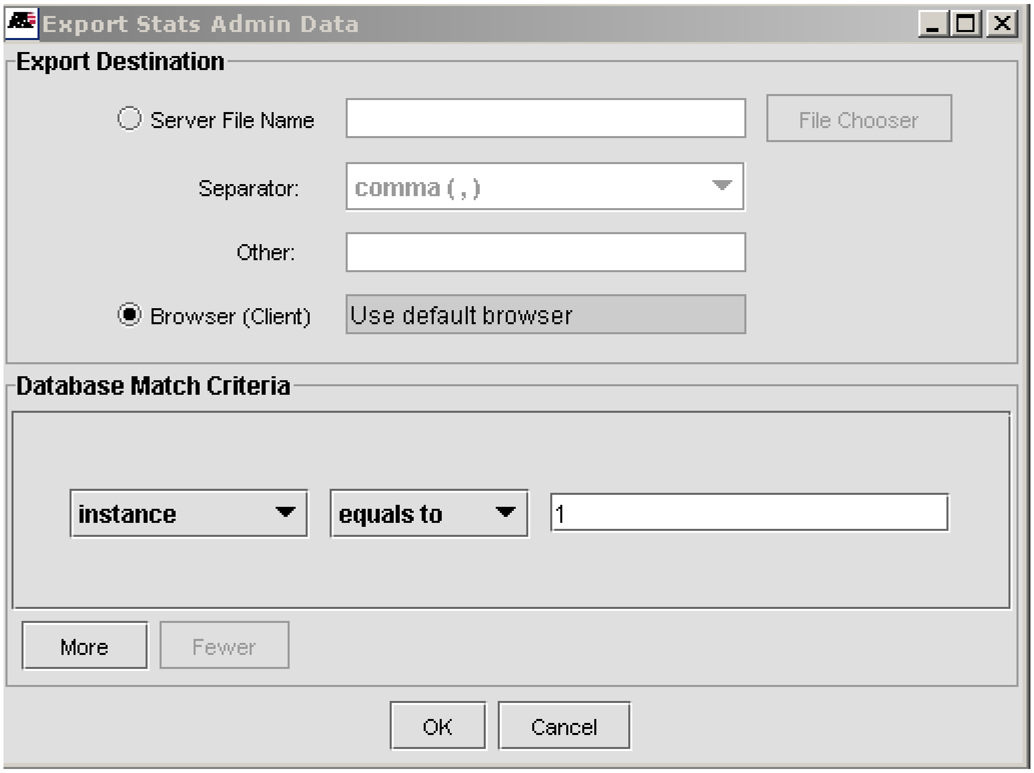


FIGURE 30-4 Viewing Instances in a Device for a Statistic

When exporting the statistical data in a table, the user can isolate this instance as part of the match criteria. The following figure shows setting up the instance criteria for the statistic and the results (in a web browser). Note that the time between each polled value is 15 seconds.



○ Server File Name

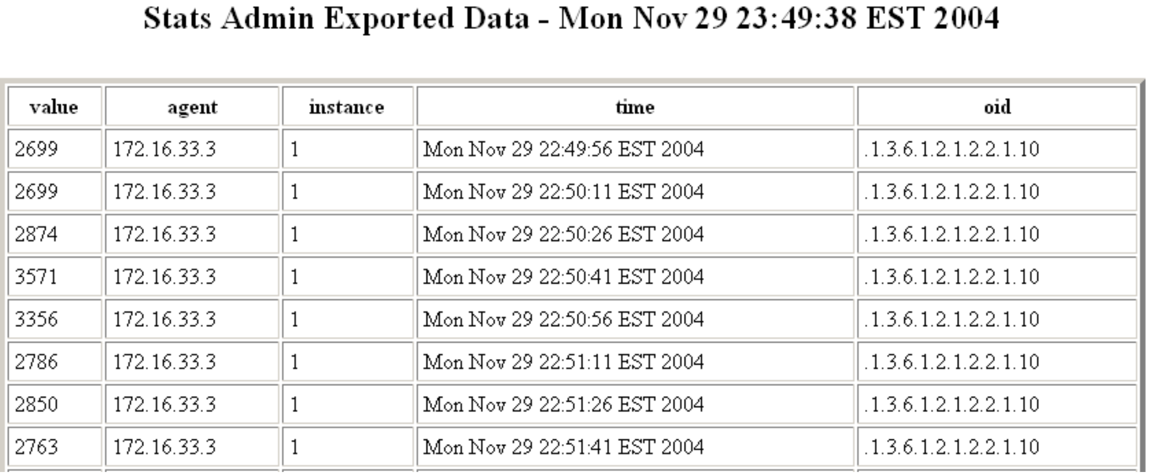
Separator: comma (,)

Other:

● Browser (Client) Use default browser

instance equals to 1

FIGURE 30-5 Setting the Criteria for Performance (Instance)



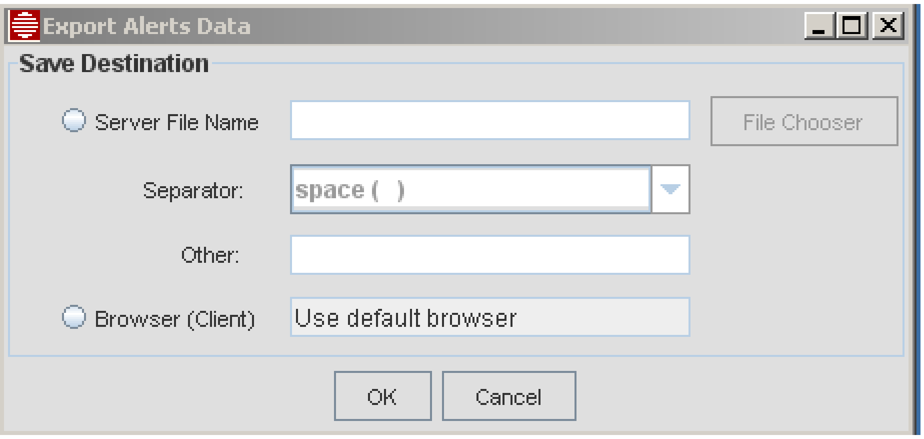
Stats Admin Exported Data - Mon Nov 29 23:49:38 EST 2004

value	agent	instance	time	oid
2699	172.16.33.3	1	Mon Nov 29 22:49:56 EST 2004	.1.3.6.1.2.1.2.2.1.10
2699	172.16.33.3	1	Mon Nov 29 22:50:11 EST 2004	.1.3.6.1.2.1.2.2.1.10
2874	172.16.33.3	1	Mon Nov 29 22:50:26 EST 2004	.1.3.6.1.2.1.2.2.1.10
3571	172.16.33.3	1	Mon Nov 29 22:50:41 EST 2004	.1.3.6.1.2.1.2.2.1.10
3356	172.16.33.3	1	Mon Nov 29 22:50:56 EST 2004	.1.3.6.1.2.1.2.2.1.10
2786	172.16.33.3	1	Mon Nov 29 22:51:11 EST 2004	.1.3.6.1.2.1.2.2.1.10
2850	172.16.33.3	1	Mon Nov 29 22:51:26 EST 2004	.1.3.6.1.2.1.2.2.1.10
2763	172.16.33.3	1	Mon Nov 29 22:51:41 EST 2004	.1.3.6.1.2.1.2.2.1.10

FIGURE 30-6 Results of Performance Statistic by Instance (15-second Intervals)

30.3 Exporting Selected Items

To export manually selected items from a data table, select the items you wish to export (use SHIFT+left-click to select multiple items), and then select *Edit* -> *Export Selected Rows* from the Panel-Specific Menu Bar. The Export Events Data form, shown in the following figure, will appear.



○ Server File Name

Separator: space ( )

Other:

○ Browser (Client) Use default browser

FIGURE 30-7 Export PhysicalLinks Data Form - Exporting Selected Data

The **Database Match Criteria** panel does not appear on this form since the items were manually selected. On this form, select a target for the exported data as described in the previous paragraphs. The resulting data file is described in the following section.

30.4 Viewing a Data Export File

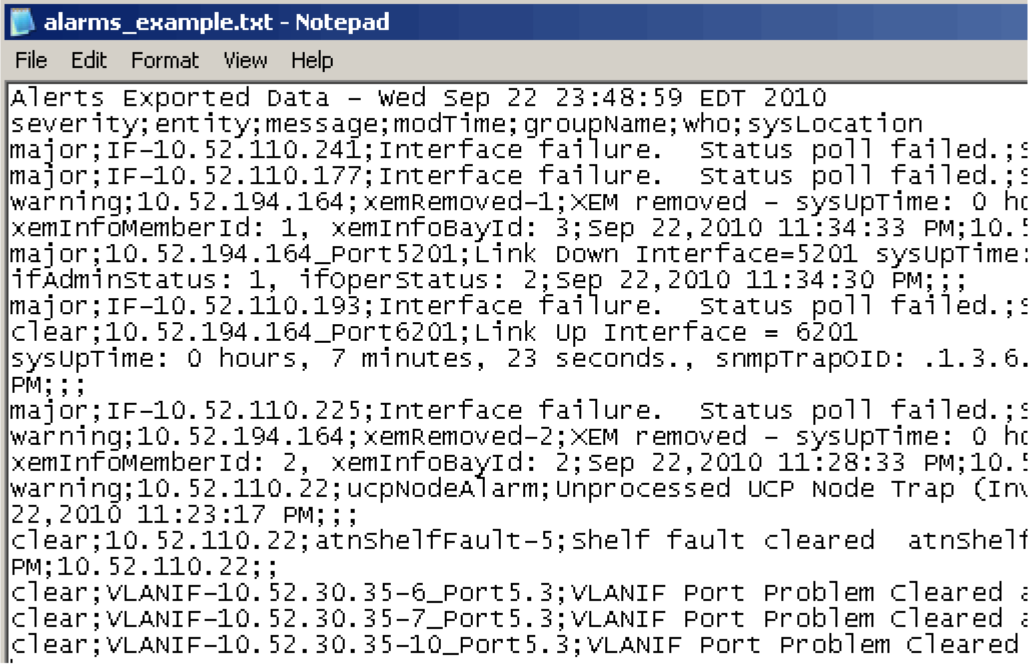
If you export table data to a file, you can access the file using your Web browser as follows:

1. Enter the following address in your Web browser Address bar:

   Input: http://<NMS_server_ip>:9090/state

   where NMS_server_ip is the IP address of the NMS Server.
2. Locate your data file. For Microsoft Internet Explorer, right-click the file. For Netscape, SHIFT+right-click the file.
3. Save the file to a directory on your local machine.
4. To view the file, open it on your local machine with any ASCII text editor, such as Notepad or vi.

An example data file is shown in the following figure. This file is the result of the data export example described previously. Notice that each field in the table is separated with a semi-colon (;), which was defined as the separator in the example.

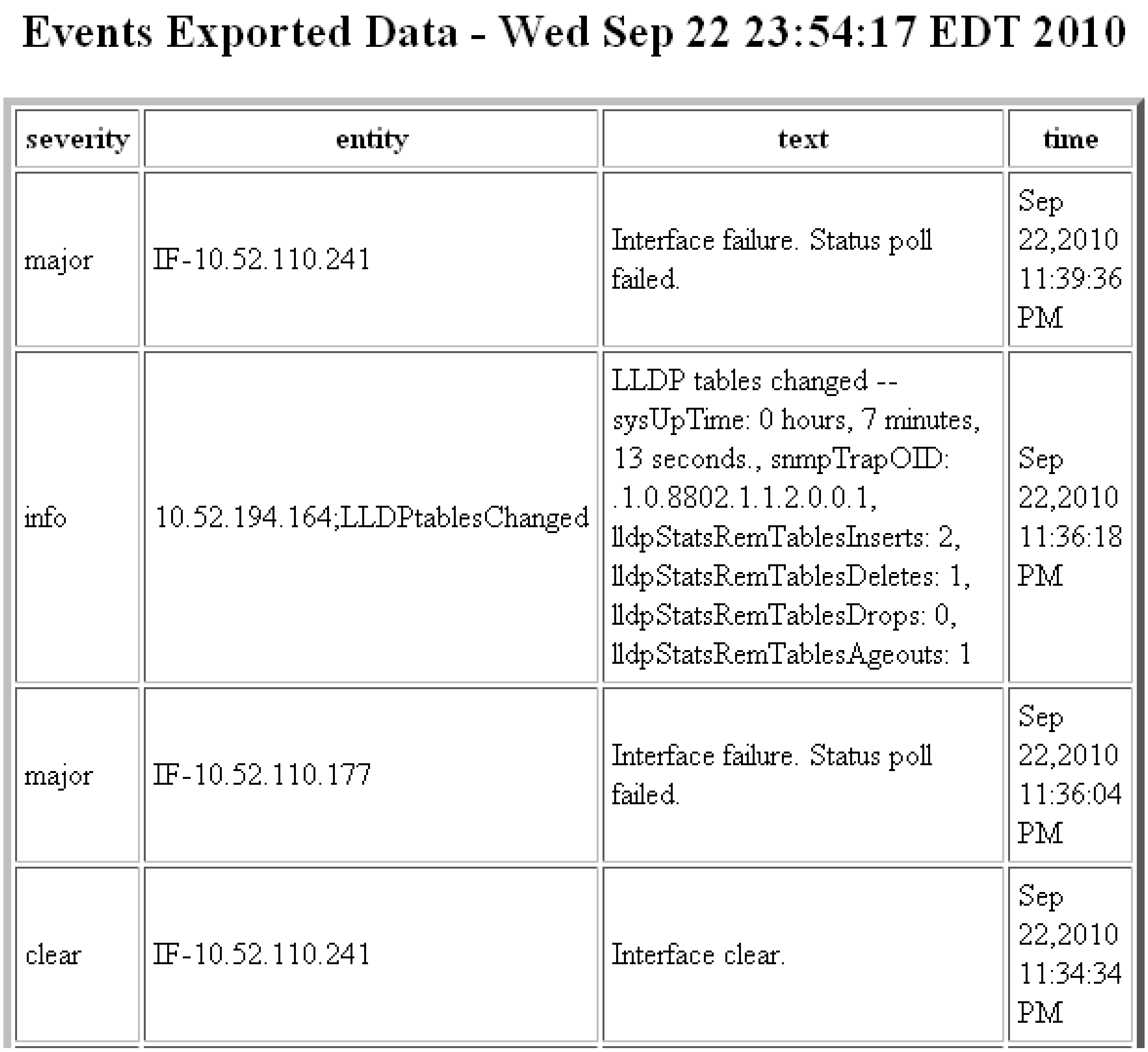


```
Alerts Exported Data - Wed Sep 22 23:48:59 EDT 2010
severity;entity;message;modTime;groupName;who;sysLocation
major;IF-10.52.110.241;Interface failure.  Status poll failed.;S
major;IF-10.52.110.177;Interface failure.  Status poll failed.;S
warning;10.52.194.164;xemRemoved-1;XEM removed - sysUpTime: 0 ho
xemInfoMemberId: 1, xemInfoBayId: 3;Sep 22,2010 11:34:33 PM;10.5
major;10.52.194.164_Port5201;Link Down Interface=5201 sysUpTime:
ifAdminStatus: 1, ifOperStatus: 2;Sep 22,2010 11:34:30 PM;;;
major;IF-10.52.110.193;Interface failure.  Status poll failed.;S
clear;10.52.194.164_Port6201;Link Up Interface = 6201
sysUpTime: 0 hours, 7 minutes, 23 seconds., snmpTrapOID: .1.3.6.
PM;;;
major;IF-10.52.110.225;Interface failure.  Status poll failed.;S
warning;10.52.194.164;xemRemoved-2;XEM removed - sysUpTime: 0 ho
xemInfoMemberId: 2, xemInfoBayId: 2;Sep 22,2010 11:28:33 PM;10.5
warning;10.52.110.22;ucpNodeAlarm;Unprocessed UCP Node Trap (Inv
22,2010 11:23:17 PM;;;
clear;10.52.110.22;atnShelfFault-5;Shelf fault cleared  atnShelf
PM;10.52.110.22;;
clear;VLANIF-10.52.30.35-6_Port5.3;VLANIF Port Problem Cleared a
clear;VLANIF-10.52.30.35-7_Port5.3;VLANIF Port Problem Cleared a
clear;VLANIF-10.52.30.35-10_Port5.3;VLANIF Port Problem Cleared
```

FIGURE 30-8 Exported Data File Example- File

30.5 Viewing Data on a Web Browser

If you exported the data to your Web browser, the data will be displayed in a new browser window. An example is shown in the following figure. You can use the menus in your Web browser to view, print, or save the information.



Events Exported Data - Wed Sep 22 23:54:17 EDT 2010

severity	entity	text	time
major	IF-10.52.110.241	Interface failure. Status poll failed.	Sep 22,2010 11:39:36 PM
info	10.52.194.164;LLDPtablesChanged	LLDP tables changed -- sysUpTime: 0 hours, 7 minutes, 13 seconds., snmpTrapOID: .1.0.8802.1.1.2.0.0.1, lldpStatsRemTablesInserts: 2, lldpStatsRemTablesDeletes: 1, lldpStatsRemTablesDrops: 0, lldpStatsRemTablesAgeouts: 1	Sep 22,2010 11:36:18 PM
major	IF-10.52.110.177	Interface failure. Status poll failed.	Sep 22,2010 11:36:04 PM
clear	IF-10.52.110.241	Interface clear.	Sep 22,2010 11:34:34 PM

FIGURE 30-9 Tabular Data Displayed in a Web Browser

31. dhcpd Files

Following is a complete example of a dhcpd file, with comments highlighted. There are five files, since DHCP-related configurations for each Access Island are placed in separate configuration files.

31.1 dhcpd.conf

```
# dhcpd.conf for Service Provider Solutions Interop (SPSI) lab
# Jul-12-08 JWS: removed subnets AI01, L2Supp, YKTA
# Jul-8-10 JWS: added subnets spsi-ai00-awplus

log-facility local7;
################################################################################
# In addition to setting this value, you may need to modify your
# syslog.conf file to configure logging of the DHCP server.
# For example, you might add a line like this:
# local7.*      /val/log/dhcpd.log
# local7.info   @10.52.110.4
################################################################################
server-name "dhcp1";
server-identifier dhcp1.spsi.lab.telesyn.corp;
authoritative;
ddns-update-style interim;
#option domain-name-servers 166.163.129.19,166.163.128.15,166.163.128.5;
default-lease-time 86400;
max-lease-time 86400;
# To identify the network that this machine is physically on.
#subnet 10.52.110.32 netmask 255.255.255.240 {
subnet 10.52.201.0 netmask 255.255.255.0 {
}

if exists agent.circuit-id
{
 if ((substring(option vendor-class-identifier,0,8)="iMG646PX") or (substring(option vendor-class-identifier,0,9)="iMG646MOD"))
 {
   log (info, concat(
    "  PX INCOMING> ",binary-to-ascii(10, 8, ".", leased-address),
    " MAC: ",binary-to-ascii(16,8,":",hardware),
    " offered to iMAP: ",(option agent.remote-id),
    " INTERFACE: ",binary-to-ascii(10, 8, ".", substring(option agent.circuit-id, 0, 3)),
    ", VLAN: ",binary-to-ascii(10, 16, "", substring(option agent.circuit-id, 3, 2))
   ));
 }
 else
 {
   log (info, concat(
    "  INCOMING> ",binary-to-ascii(10, 8, ".", leased-address),
    " MAC: ",binary-to-ascii(16,8,":",hardware),
    " offered to iMAP: ",(option agent.remote-id),
    " INTERFACE: ",binary-to-ascii(10, 8, ".", substring(option agent.circuit-id, 0, 2)),
    ", VLAN: ",binary-to-ascii(10, 16, "", substring(option agent.circuit-id, 2, 2))
   ));
 }
}

#log ( info, concat(
#">>Lease for ",binary-to-ascii(10, 8, ".", leased-address),
#" raw option-82 info is CID: ",binary-to-ascii(10, 8, ".", option agent.circuit-id),
#" AID: ",binary-to-ascii(16, 8, ".", option agent.remote-id)
# ));


on commit
{
 if ((substring(option vendor-class-identifier,0,8)="iMG646PX") or (substring(option vendor-class-identifier,0,9)="iMG646MOD"))
 {
  log (info, concat(
   " LEASE ACK>> ",binary-to-ascii(10, 8, ".", leased-address),
   " MAC: ",binary-to-ascii(16,8,":",hardware),
   " linked & associated to iMAP: ",(option agent.remote-id),
   " INTERFACE: ",binary-to-ascii(10, 8, ".", substring(option agent.circuit-id, 0, 3)),
   ", VLAN: ",binary-to-ascii(10, 16, "", substring(option agent.circuit-id, 3, 2))
  ));
 }
 else
 {
  log (info, concat(
  " LEASE ACK>> ",binary-to-ascii(10, 8, ".", leased-address),
  " MAC: ",binary-to-ascii(16,8,":",hardware),
  " linked & associated to iMAP: ",(option agent.remote-id),
  " INTERFACE: ",binary-to-ascii(10, 8, ".", substring(option agent.circuit-id, 0, 2)),
  ", VLAN: ",binary-to-ascii(10, 16, "", substring(option agent.circuit-id, 2, 2))
  ));
 }
}


on expiry
{
 if ((substring(option vendor-class-identifier,0,8)="iMG646PX") or (substring(option vendor-class-identifier,0,9)="iMG646MOD"))
 {
  log (info, concat(
  " LEASE EXPIRE>> ",binary-to-ascii(10, 8, ".", leased-address),
  " MAC: ",binary-to-ascii(16,8,":",hardware),
  " associated to iMAP: ",(option agent.remote-id),
  " INTERFACE: ",binary-to-ascii(10, 8, ".", substring(option agent.circuit-id, 0, 2)),
  ", VLAN: ",binary-to-ascii(10, 16, "", substring(option agent.circuit-id, 2, 2))
  ));
 }
 else
 {
  log (info, concat(
  " LEASE EXPIRE>> ",binary-to-ascii(10, 8, ".", leased-address),
  " MAC: ",binary-to-ascii(16,8,":",hardware),
  " associated to iMAP: ",(option agent.remote-id),
  " INTERFACE: ",binary-to-ascii(10, 8, ".", substring(option agent.circuit-id, 0, 2)),
  ", VLAN: ",binary-to-ascii(10, 16, "", substring(option agent.circuit-id, 2, 2))
  ));
 }
}

on release
{
 if ((substring(option vendor-class-identifier,0,8)="iMG646PX") or (substring(option vendor-class-identifier,0,9)="iMG646MOD"))
 {
  log (info, concat(
  "  RELEASE> ",binary-to-ascii(10, 8, ".", leased-address),
  " MAC: ",binary-to-ascii(16,8,":",hardware),
  " released on iMAP: ",(option agent.remote-id),
  " INTERFACE: ",binary-to-ascii(10, 8, ".", substring(option agent.circuit-id, 0, 2)),
  " VLAN: ",binary-to-ascii(10, 16, "", substring(option agent.circuit-id, 2, 2))
  ));
 }
 else
 {
  log (info, concat(
  "  RELEASE> ",binary-to-ascii(10, 8, ".", leased-address),
  " MAC: ",binary-to-ascii(16,8,":",hardware),
  " released on iMAP: ",(option agent.remote-id),
  " INTERFACE: ",binary-to-ascii(10, 8, ".", substring(option agent.circuit-id, 0, 2)),
  ", VLAN: ",binary-to-ascii(10, 16, "", substring(option agent.circuit-id, 2, 2))
  ));
 }
}

# STB class config files
include "/etc/dhcpd_include/vendor-amino.conf";
include "/etc/dhcpd_include/class-stb.conf";

# MAP class config files
include "/etc/dhcpd_include/spsi-ai00-class";
include "/etc/dhcpd_include/spsi-ai00-awplus-class";

# MAP subnet config files
include "/etc/dhcpd_include/spsi-ai00-subnet";
include "/etc/dhcpd_include/spsi-ai00-awplus-subnet";
```

31.2 dhcpd Includes

31.2.1 spsi-ai00-class

```
# spsi-ai00-class for Service Provider Solutions Interop (SPSI) lab Access Island 0
# Jul-15-08 JWS: modified for migration of nms server ip from 10.52.110.4 to 10.52.201.4
# Jul-22-08 JWS: modified for iMG634A-R2 (ODM)
# Feb-12-09 JWS: modified to add iMG613RF, iMG616BD
# Feb-13-09 JWS: modified to add iMG606BD
# Mar-31-09 JWS: modified to add iMG726MOD, iMG746MOD
# Jul-22-09 JWS: modified to add iMG616W
# Oct-9-09 JWS: modified for iMG624A-R2
# Oct-22-09 JWS: modified for Comtrend NexusLink 5631 ADSL bonded CPE
# Dec-4-09 JWS: modified rg613tx boot path
# Feb-12-10 JWS: modified to completely add iMG634WA
# Jul-7-10 JWS: corrected boot file path for iMG7x6MOD
# Dec-14-10 JWS: modified to add video class for iMGs
# Apr-7-11 JWS: added iMG726BD-ON
# May-4-11 JWS: added iMG606BD-R2
# May-19-11 JWS: added iMG616BD-R2, removed img's that don't support voice from voice section, other clean up
# Jun-8-11 JWS: added iMG613RF voice
# Aug-1-11 JWS: added iMG2504
# Aug-4-11 JWS: added iMG1525
# Oct-6-11 JWS: added iMG1505
# Dec-2-11 JWS: added iMG2524, removed img1505 and img2504 from voice section

##################################################################################

# AGENT REMOTE ID:

# SPSI-AI00  (TEST [AI00] ACCESS ISLAND)  #

# AGENT CIRCUIT ID:

# Vlan 100 (MAPMgmt)    = \x00\x64      = 10.52.110.16   255.255.255.240 nonUFO

# Vlan 200 (RGBoot)    = \x00\xc8      = 10.52.111.0    255.255.255.192 UFO

# Vlan 300 (RGMgmt)     = \x01\x2c      = 10.52.111.64   255.255.255.192 UFO

# Vlan 400 (Voice)      = \x01\x90      = 10.52.111.128  255.255.255.192 UFO

# Vlan 500 (Video)      = \x01\xf4      = 10.52.111.192  255.255.255.192 UFO

# Vlan 600 (Internet)   = \x02\x58      = 10.52.110.64   255.255.252.224 UFO?

##################################################################################

### RG Mgmt vlan 300 ###

class "SPSI-AI00-RG613TXMgmt" {

  match if ((substring(option agent.remote-id,0,9)="SPSI-AI00") and (substring(option agent.circuit-id,2,2)="\x01\x2c") and

    (option vendor-class-identifier = "RG613TX"));

      option vendor-class-identifier "RG613TX";

}

class "SPSI-AI00-RG624AMgmt" {

  match if ((substring(option agent.remote-id,0,9)="SPSI-AI00") and (substring(option agent.circuit-id,2,2)="\x01\x2c") and

    (option vendor-class-identifier = "RG624A"));

      option vendor-class-identifier "RG624A";

}

class "SPSI-AI00-RG634AMgmt" {

  match if ((substring(option agent.remote-id,0,9)="SPSI-AI00") and (substring(option agent.circuit-id,2,2)="\x01\x2c") and

    (option vendor-class-identifier = "RG634A"));

      option vendor-class-identifier "RG634A";

}

class "SPSI-AI00-iMG606BDMgmt" {

  match if ((substring(option agent.remote-id,0,9)="SPSI-AI00") and (substring(option agent.circuit-id,2,2)="\x01\x2c") and

    (option vendor-class-identifier = "iMG606BD"));

      option vendor-class-identifier "iMG606BD";

}

class "SPSI-AI00-iMG606BD-R2Mgmt" {

  match if ((substring(option agent.remote-id,0,9)="SPSI-AI00") and (substring(option agent.circuit-id,2,2)="\x01\x2c") and

    (option vendor-class-identifier = "iMG606BD-R2"));

      option vendor-class-identifier "iMG606BD-R2";

}

class "SPSI-AI00-iMG613RFMgmt" {

  match if ((substring(option agent.remote-id,0,9)="SPSI-AI00") and (substring(option agent.circuit-id,2,2)="\x01\x2c") and
    (option vendor-class-identifier = "iMG613RF"));
      option vendor-class-identifier "iMG613RF";
}
class "SPSI-A100-iMG616BDMgmt" {
  match if ((substring(option agent.remote-id,0,9)="SPSI-A100") and (substring(option agent.circuit-id,2,2)="\x01\x2c") and
    (option vendor-class-identifier = "iMG616BD"));
      option vendor-class-identifier "iMG616BD";
}
class "SPSI-A100-iMG616BD-R2Mgmt" {
  match if ((substring(option agent.remote-id,0,9)="SPSI-A100") and (substring(option agent.circuit-id,2,2)="\x01\x2c") and
    (option vendor-class-identifier = "iMG616BD-R2"));
      option vendor-class-identifier "iMG616BD-R2";
}
class "SPSI-A100-iMG616WMgmt" {
  match if ((substring(option agent.remote-id,0,9)="SPSI-A100") and (substring(option agent.circuit-id,2,2)="\x01\x2c") and
    (option vendor-class-identifier = "iMG616W"));
      option vendor-class-identifier "iMG616W";
}
class "SPSI-A100-iMG624AMgmt" {
  match if ((substring(option agent.remote-id,0,9)="SPSI-A100") and (substring(option agent.circuit-id,2,2)="\x01\x2c") and
    (option vendor-class-identifier = "iMG624A"));
      option vendor-class-identifier "iMG624A";
}
class "SPSI-A100-iMG624A-R2Mgmt" {
  match if ((substring(option agent.remote-id,0,9)="SPSI-A100") and (substring(option agent.circuit-id,2,2)="\x01\x2c") and
    (option vendor-class-identifier = "iMG624A-R2"));
      option vendor-class-identifier "iMG624A-R2";
}
class "SPSI-A100-iMG634AMgmt" {
  match if ((substring(option agent.remote-id,0,9)="SPSI-A100") and (substring(option agent.circuit-id,2,2)="\x01\x2c") and
    (option vendor-class-identifier = "iMG634A"));
      option vendor-class-identifier "iMG634A";
}
class "SPSI-A100-iMG634A-R2Mgmt" {
  match if ((substring(option agent.remote-id,0,9)="SPSI-A100") and (substring(option agent.circuit-id,2,2)="\x01\x2c") and
    (option vendor-class-identifier = "iMG634A-R2"));
      option vendor-class-identifier "iMG634A-R2";
}
class "SPSI-A100-iMG634WAMgmt" {
  match if ((substring(option agent.remote-id,0,9)="SPSI-A100") and (substring(option agent.circuit-id,2,2)="\x01\x2c") and
    (option vendor-class-identifier = "iMG634WA"));
      option vendor-class-identifier "iMG634WA";
}
class "SPSI-A100-iMG646BDMgmt" {
  match if ((substring(option agent.remote-id,0,9)="SPSI-A100") and (substring(option agent.circuit-id,2,2)="\x01\x2c") and
    (option vendor-class-identifier = "iMG646BD"));
      option vendor-class-identifier "iMG646BD";
}
class "SPSI-A100-iMG646BD-ONMgmt" {
  match if ((substring(option agent.remote-id,0,9)="SPSI-A100") and (substring(option agent.circuit-id,2,2)="\x01\x2c") and
    (option vendor-class-identifier = "iMG646BD-ON"));
      option vendor-class-identifier "iMG646BD-ON";
}
class "SPSI-A100-iMG626MODMgmt" {
  match if ((substring(option agent.remote-id,0,9)="SPSI-A100") and
    ((substring(option agent.circuit-id,2,2)="\x01\x2c") or (substring(option agent.circuit-id,3,2)="\x01\x2c")) and
    (option vendor-class-identifier = "iMG626MOD"));
      option vendor-class-identifier "iMG626MOD";
}
class "SPSI-A100-iMG646MODMgmt" {
  match if ((substring(option agent.remote-id,0,9)="SPSI-A100") and
    ((substring(option agent.circuit-id,2,2)="\x01\x2c") or (substring(option agent.circuit-id,3,2)="\x01\x2c")) and
    (option vendor-class-identifier = "iMG646MOD"));
      option vendor-class-identifier "iMG646MOD";
}
class "SPSI-A100-iMG646PX-ONMgmt" {
  match if ((substring(option agent.remote-id,0,9)="SPSI-A100") and (substring(option agent.circuit-id,3,2)="\x01\x2c") and
    (option vendor-class-identifier = "iMG646PX-ON"));
      option vendor-class-identifier "iMG646PX-ON";
}
class "SPSI-A100-iMG726BD-ONMgmt" {
  match if ((substring(option agent.remote-id,0,9)="SPSI-A100") and (substring(option agent.circuit-id,2,2)="\x01\x2c") and
    (option vendor-class-identifier = "iMG726BD-ON"));
      option vendor-class-identifier "iMG726BD-ON";
}
class "SPSI-A100-iMG726MODMgmt" {
  match if ((substring(option agent.remote-id,0,9)="SPSI-A100") and
    ((substring(option agent.circuit-id,2,2)="\x01\x2c") or (substring(option agent.circuit-id,3,2)="\x01\x2c")) and
    (option vendor-class-identifier = "iMG726MOD"));
      option vendor-class-identifier "iMG726MOD";
}
class "SPSI-A100-iMG746MODMgmt" {
  match if ((substring(option agent.remote-id,0,9)="SPSI-A100") and
    ((substring(option agent.circuit-id,2,2)="\x01\x2c") or (substring(option agent.circuit-id,3,2)="\x01\x2c")) and
    (option vendor-class-identifier = "iMG746MOD"));
      option vendor-class-identifier "iMG746MOD";
}
class "SPSI-A100-iBG915FXMgmt" {
  match if ((substring(option agent.remote-id,0,9)="SPSI-A100") and (substring(option agent.circuit-id,2,2)="\x01\x2c") and
    (option vendor-class-identifier = "iBG915FX"));
      option vendor-class-identifier "iBG915FX";
}
```

```
class "SPSI-AI00-iMG1505Mgmt" {
  match if ((substring(option agent.remote-id,0,9)="SPSI-AI00") and (substring(option agent.circuit-id,2,2)="\x01\x2c") and
    (option vendor-class-identifier = "iMG1505"));
      option vendor-class-identifier "iMG1505";
}
class "SPSI-AI00-iMG1525Mgmt" {
  match if ((substring(option agent.remote-id,0,9)="SPSI-AI00") and (substring(option agent.circuit-id,2,2)="\x01\x2c") and
    (option vendor-class-identifier = "iMG1525"));
      option vendor-class-identifier "iMG1525";
}
class "SPSI-AI00-iMG2504Mgmt" {
  match if ((substring(option agent.remote-id,0,9)="SPSI-AI00") and (substring(option agent.circuit-id,2,2)="\x01\x2c") and
    (option vendor-class-identifier = "iMG2504"));
      option vendor-class-identifier "iMG2504";
}
class "SPSI-AI00-iMG2524Mgmt" {
  match if ((substring(option agent.remote-id,0,9)="SPSI-AI00") and (substring(option agent.circuit-id,2,2)="\x01\x2c") and
    (option vendor-class-identifier = "iMG2524"));
      option vendor-class-identifier "iMG2524";
}
class "SPSI-AI00-ComtrendMgmt"
{
  match if
    (substring
      (option agent.remote-id,0,9)
    ="SPSI-AI00")
  and
    (substring
      (option agent.circuit-id,2,2)
    ="\x01\x2c")
  and
    (substring
      (option vendor-class-identifier,0,5)
    ="uDHCP")
   ;
#  option bootfile-name "10.52.201.4";
}


### RG Boot vlan 200 ###
class "SPSI-AI00-RG613TXBoot" {
  match if ((substring(option agent.remote-id,0,9)="SPSI-AI00") and (substring(option agent.circuit-id,2,2)="\x00\xc8") and
    (option vendor-class-identifier = "RG613TX"));
      filename "FIBER/AI00/RG613TX";
      option tftp-server-name "10.52.201.4";
      option vendor-class-identifier "RG613TX";
}
class "SPSI-AI00-RG624ABoot" {
  match if ((substring(option agent.remote-id,0,9)="SPSI-AI00") and (substring(option agent.circuit-id,2,2)="\x00\xc8") and
    (option vendor-class-identifier = "RG624A"));
      filename "ADSL/AI00/RG600A";
      option tftp-server-name "10.52.201.4";
      option vendor-class-identifier "RG624A";
}
class "SPSI-AI00-RG634ABoot" {
  match if ((substring(option agent.remote-id,0,9)="SPSI-AI00") and (substring(option agent.circuit-id,2,2)="\x00\xc8") and
    (option vendor-class-identifier = "RG634A"));
      filename "ADSL/AI00/RG600A";
      option tftp-server-name "10.52.201.4";
      option vendor-class-identifier "RG634A";
}
class "SPSI-AI00-iMG606BDBoot" {
  match if ((substring(option agent.remote-id,0,9)="SPSI-AI00") and (substring(option agent.circuit-id,2,2)="\x00\xc8") and
    (option vendor-class-identifier = "iMG606BD"));
       filename "FIBER/AI00/IMG6XX";
       option tftp-server-name "10.52.201.4";
       option vendor-class-identifier "iMG606BD";
}
class "SPSI-AI00-iMG606BD-R2Boot" {
  match if ((substring(option agent.remote-id,0,9)="SPSI-AI00") and (substring(option agent.circuit-id,2,2)="\x00\xc8") and
    (option vendor-class-identifier = "iMG606BD-R2"));
       filename "FIBER/AI00/IMG606BD-R2";
       option tftp-server-name "10.52.201.4";
       option vendor-class-identifier "iMG606BD-R2";
}
class "SPSI-AI00-iMG613RFBoot" {
  match if ((substring(option agent.remote-id,0,9)="SPSI-AI00") and (substring(option agent.circuit-id,2,2)="\x00\xc8") and
    (option vendor-class-identifier = "iMG613RF"));
       filename "FIBER/AI00/IMG600";
       option tftp-server-name "10.52.201.4";
       option vendor-class-identifier "iMG613RF";
}
class "SPSI-AI00-iMG616BDBoot" {
  match if ((substring(option agent.remote-id,0,9)="SPSI-AI00") and (substring(option agent.circuit-id,2,2)="\x00\xc8") and
    (option vendor-class-identifier = "iMG616BD"));
       filename "FIBER/AI00/IMG616";
       option tftp-server-name "10.52.201.4";
       option vendor-class-identifier "iMG616BD";
}
class "SPSI-AI00-iMG616BD-R2Boot" {
  match if ((substring(option agent.remote-id,0,9)="SPSI-AI00") and (substring(option agent.circuit-id,2,2)="\x00\xc8") and
    (option vendor-class-identifier = "iMG616BD-R2"));
       filename "FIBER/AI00/IMG616BD-R2";
       option tftp-server-name "10.52.201.4";
       option vendor-class-identifier "iMG616BD-R2";
}
class "SPSI-AI00-iMG616WBoot" {
  match if ((substring(option agent.remote-id,0,9)="SPSI-AI00") and (substring(option agent.circuit-id,2,2)="\x00\xc8") and
    (option vendor-class-identifier = "iMG616W"));
       filename "FIBER/AI00/IMG616W";
       option tftp-server-name "10.52.201.4";
       option vendor-class-identifier "iMG616W";
}
class "SPSI-A100-iMG624ABoot" {
  match if ((substring(option agent.remote-id,0,9)="SPSI-A100") and (substring(option agent.circuit-id,2,2)="\x00\xc8") and
    (option vendor-class-identifier = "iMG624A"));
      filename "ADSL/A100/IMG624A";
      option tftp-server-name "10.52.201.4";
      option vendor-class-identifier "iMG624A";
}
class "SPSI-A100-iMG624A-R2Boot" {
  match if ((substring(option agent.remote-id,0,9)="SPSI-A100") and (substring(option agent.circuit-id,2,2)="\x00\xc8") and
    (option vendor-class-identifier = "iMG624A-R2"));
      filename "ADSL/A100/iMG624A-R2";
      option tftp-server-name "10.52.201.4";
      option vendor-class-identifier "iMG624A-R2";
}
class "SPSI-A100-iMG634ABoot" {
  match if ((substring(option agent.remote-id,0,9)="SPSI-A100") and (substring(option agent.circuit-id,2,2)="\x00\xc8") and
    (option vendor-class-identifier = "iMG634A"));
      filename "ADSL/A100/IMG634A";
      option tftp-server-name "10.52.201.4";
      option vendor-class-identifier "iMG634A";
}
class "SPSI-A100-iMG634A-R2Boot" {
  match if ((substring(option agent.remote-id,0,9)="SPSI-A100") and (substring(option agent.circuit-id,2,2)="\x00\xc8") and
    (option vendor-class-identifier = "iMG634A-R2"));
      filename "ADSL/A100/IMG634A-R2";
      option tftp-server-name "10.52.201.4";
      option vendor-class-identifier "iMG634A-R2";
}
class "SPSI-A100-iMG634WABoot" {
  match if ((substring(option agent.remote-id,0,9)="SPSI-A100") and (substring(option agent.circuit-id,2,2)="\x00\xc8") and
    (option vendor-class-identifier = "iMG634WA"));
      filename "ADSL/A100/IMG634WA";
      option tftp-server-name "10.52.201.4";
      option vendor-class-identifier "iMG634WA";
}
class "SPSI-A100-iMG646BDBoot" {
  match if ((substring(option agent.remote-id,0,9)="SPSI-A100") and (substring(option agent.circuit-id,2,2)="\x00\xc8") and
    (option vendor-class-identifier = "iMG646BD"));
       filename "FIBER/A100/IMG6XX";
       option tftp-server-name "10.52.201.4";
       option vendor-class-identifier "iMG646BD";
}
```

```
class "SPSI-AI00-iMG646BD-ONBoot" {

  match if ((substring(option agent.remote-id,0,9)="SPSI-AI00") and (substring(option agent.circuit-id,2,2)="\x00\xc8") and

    (option vendor-class-identifier = "iMG646BD-ON"));

       filename "FIBER/AI00/IMG6XX";

       option tftp-server-name "10.52.201.4";

       option vendor-class-identifier "iMG646BD-ON";

}

class "SPSI-AI00-iMG626MODBoot" {

  match if ((substring(option agent.remote-id,0,9)="SPSI-AI00") and
    ((substring(option agent.circuit-id,2,2)="\x00\xc8") or (substring(option agent.circuit-id,3,2)="\x00\xc8")) and

    (option vendor-class-identifier = "iMG626MOD"));

      filename "FIBER/AI00/IMG626MOD";

      option tftp-server-name "10.52.201.4";

      option vendor-class-identifier "iMG626MOD";

}

class "SPSI-AI00-iMG646MODBoot" {

  match if ((substring(option agent.remote-id,0,9)="SPSI-AI00") and
    ((substring(option agent.circuit-id,2,2)="\x00\xc8") or (substring(option agent.circuit-id,3,2)="\x00\xc8")) and

    (option vendor-class-identifier = "iMG646MOD"));

      filename "FIBER/AI00/IMG646MOD";

      option tftp-server-name "10.52.201.4";

      option vendor-class-identifier "iMG646MOD";

}

class "SPSI-AI00-iMG646PX-ONBoot" {

  match if ((substring(option agent.remote-id,0,9)="SPSI-AI00") and (substring(option agent.circuit-id,3,2)="\x00\xc8") and

    (option vendor-class-identifier = "iMG646PX-ON"));

      filename "FIBER/AI00/IMG6XX";

      option tftp-server-name "10.52.201.4";

      option vendor-class-identifier "iMG646PX-ON";

}

class "SPSI-AI00-iMG726BD-ONBoot" {

  match if ((substring(option agent.remote-id,0,9)="SPSI-AI00") and (substring(option agent.circuit-id,2,2)="\x00\xc8") and

    (option vendor-class-identifier = "iMG726BD-ON"));

      filename "FIBER/AI00/IMG726BD-ON";

      option tftp-server-name "10.52.201.4";

      option vendor-class-identifier "iMG726BD-ON";

}

class "SPSI-AI00-iMG726MODBoot" {

  match if ((substring(option agent.remote-id,0,9)="SPSI-AI00") and
    ((substring(option agent.circuit-id,2,2)="\x00\xc8") or (substring(option agent.circuit-id,3,2)="\x00\xc8")) and

    (option vendor-class-identifier = "iMG726MOD"));

      filename "FIBER/AI00/IMG726MOD";

      option tftp-server-name "10.52.201.4";

      option vendor-class-identifier "iMG726MOD";

}

class "SPSI-AI00-iMG746MODBoot" {
  match if ((substring(option agent.remote-id,0,9)="SPSI-A100") and
    ((substring(option agent.circuit-id,2,2)="\x00\xc8") or (substring(option agent.circuit-id,3,2)="\x00\xc8")) and
    (option vendor-class-identifier = "iMG746MOD"));
      filename "FIBER/A100/IMG746MOD";
      option tftp-server-name "10.52.201.4";
      option vendor-class-identifier "iMG746MOD";
}
class "SPSI-A100-iBG915FXBoot" {
  match if ((substring(option agent.remote-id,0,9)="SPSI-A100") and (substring(option agent.circuit-id,2,2)="\x00\xc8") and
    (option vendor-class-identifier = "iBG915FX"));
      filename "FIBER/A100/IBG915FX";
      option tftp-server-name "10.52.201.4";
      option vendor-class-identifier "iBG915FX";
}
class "SPSI-A100-iMG1505Boot" {
  match if ((substring(option agent.remote-id,0,9)="SPSI-A100") and (substring(option agent.circuit-id,2,2)="\x00\xc8") and
    (option vendor-class-identifier = "iMG1505"));
      filename "FIBER/A100/IMG1505";
      option tftp-server-name "10.52.201.4";
      option vendor-class-identifier "iMG1505";
}
class "SPSI-A100-iMG1525Boot" {
  match if ((substring(option agent.remote-id,0,9)="SPSI-A100") and (substring(option agent.circuit-id,2,2)="\x00\xc8") and
    (option vendor-class-identifier = "iMG1525"));
      filename "FIBER/A100/IMG1525";
      option tftp-server-name "10.52.201.4";
      option vendor-class-identifier "iMG1525";
}
class "SPSI-A100-iMG2504Boot" {
  match if ((substring(option agent.remote-id,0,9)="SPSI-A100") and (substring(option agent.circuit-id,2,2)="\x00\xc8") and
    (option vendor-class-identifier = "iMG2504"));
      filename "FIBER/A100/IMG2504";
      option tftp-server-name "10.52.201.4";
      option vendor-class-identifier "iMG2504";
}
class "SPSI-A100-iMG2524Boot" {
  match if ((substring(option agent.remote-id,0,9)="SPSI-A100") and (substring(option agent.circuit-id,2,2)="\x00\xc8") and
    (option vendor-class-identifier = "iMG2524"));
      filename "FIBER/A100/iMG2524";
      option tftp-server-name "10.52.201.4";
      option vendor-class-identifier "iMG2524";
}
### RG VoIP vlan 400 ###
class "SPSI-A100-VoIP" {
  match if (
    (
    (substring (option agent.remote-id,0,9)="SPSI-A100") and
    (substring (option agent.circuit-id,2,2)="\x01\x90") and
    (substring(option vendor-class-identifier,0,8)="iMG646BD")
   )
  or
   (
    (substring (option agent.remote-id,0,9)="SPSI-A100") and
    (substring (option agent.circuit-id,2,2)="\x01\x90") and
    (substring(option vendor-class-identifier,0,2)="RG")
   )
  or
   (
    (substring (option agent.remote-id,0,9)="SPSI-A100") and
    (substring (option agent.circuit-id,2,2)="\x01\x90") and
    (substring(option vendor-class-identifier,0,8)="iMG613RF")
   )
  or
   (
    (substring (option agent.remote-id,0,9)="SPSI-A100") and
    (substring (option agent.circuit-id,2,2)="\x01\x90") and
    (substring(option vendor-class-identifier,0,8)="iMG616BD")
   )
  or
   (
    (substring (option agent.remote-id,0,9)="SPSI-A100") and
    (substring (option agent.circuit-id,2,2)="\x01\x90") and
    (substring(option vendor-class-identifier,0,11)="iMG616BD-R2")
   )
  or
   (
    (substring (option agent.remote-id,0,9)="SPSI-A100") and
    (substring (option agent.circuit-id,2,2)="\x01\x90") and
    (substring(option vendor-class-identifier,0,8)="iMG616W")
   )
  or
   (
    (substring (option agent.remote-id,0,9)="SPSI-A100") and
    (substring (option agent.circuit-id,2,2)="\x01\x90") and
    (substring(option vendor-class-identifier,0,7)="iMG634A")
   )
  or
   (
    (substring (option agent.remote-id,0,9)="SPSI-A100") and
    (substring (option agent.circuit-id,2,2)="\x01\x90") and
    (substring(option vendor-class-identifier,0,8)="iMG634WA")
   )
  or
   (
    (substring (option agent.remote-id,0,9)="SPSI-AI00") and
    (substring (option agent.circuit-id,3,2)="\x01\x90") and
    (substring(option vendor-class-identifier,0,8)="iMG646PX")
   )
  or
   (
    (substring (option agent.remote-id,0,9)="SPSI-AI00") and
    ((substring (option agent.circuit-id,2,2)="\x01\x90") or (substring (option agent.circuit-id,3,2)="\x01\x90")) and
    (substring(option vendor-class-identifier,0,9)="iMG626MOD")
   )
  or
   (
    (substring (option agent.remote-id,0,9)="SPSI-AI00") and
    ((substring (option agent.circuit-id,2,2)="\x01\x90") or (substring (option agent.circuit-id,3,2)="\x01\x90")) and
    (substring(option vendor-class-identifier,0,9)="iMG646MOD")
   )
  or
   (
    (substring (option agent.remote-id,0,9)="SPSI-AI00") and
    (substring (option agent.circuit-id,2,2)="\x01\x90") and
    (substring(option vendor-class-identifier,0,11)="iMG726BD-ON")
   )
  or
   (
    (substring (option agent.remote-id,0,9)="SPSI-AI00") and
    ((substring (option agent.circuit-id,2,2)="\x01\x90") or (substring (option agent.circuit-id,3,2)="\x01\x90")) and
    (substring(option vendor-class-identifier,0,9)="iMG726MOD")
   )
  or
   (
    (substring (option agent.remote-id,0,9)="SPSI-AI00") and
    ((substring (option agent.circuit-id,2,2)="\x01\x90") or (substring (option agent.circuit-id,3,2)="\x01\x90")) and
    (substring(option vendor-class-identifier,0,9)="iMG746MOD")
   )
  or
   (
    (substring (option agent.remote-id,0,9)="SPSI-AI00") and
    (substring (option agent.circuit-id,2,2)="\x01\x90") and
    (substring(option vendor-class-identifier,0,8)="iBG915FX")
   )
  or
   (
     (substring (option agent.remote-id,0,9)="SPSI-AI00") and

     (substring (option agent.circuit-id,2,2)="\x01\x90") and

     (substring(option vendor-class-identifier,0,7)="iMG1525")

    )

  or

    (

     (substring (option agent.remote-id,0,9)="SPSI-AI00") and

     (substring (option agent.circuit-id,2,2)="\x01\x90") and

     (substring(option vendor-class-identifier,0,7)="iMG2524")

    )

  );

}

### RG Video vlan 500 ###

class "SPSI-AI00-Video" {

  match if (
    (
     (substring (option agent.remote-id,0,9)="SPSI-AI00") and

     (substring (option agent.circuit-id,2,2)="\x01\xf4") and

     (
       (substring(option vendor-class-identifier,0,11)="iMG606BD-R2") or
       (substring(option vendor-class-identifier,0,11)="iMG616BD-R2") or
       (substring(option vendor-class-identifier,0,11)="iMG726BD-ON") or
       (substring(option vendor-class-identifier,0,7)="iMG1505") or
       (substring(option vendor-class-identifier,0,7)="iMG1525") or
       (substring(option vendor-class-identifier,0,7)="iMG2504") or
       (substring(option vendor-class-identifier,0,7)="iMG2524")
     )
    )
  or
    (
     (substring (option agent.remote-id,0,9)="SPSI-AI00") and

     ((substring (option agent.circuit-id,2,2)="\x01\xf4") or (substring (option agent.circuit-id,3,2)="\x01\xf4")) and

     (
       (substring(option vendor-class-identifier,0,9)="iMG726MOD") or
       (substring(option vendor-class-identifier,0,9)="iMG746MOD")
     )
    )
  );
}


### Internet vlan 600 ###

class "SPSI-AI00-Internet" {

 match if (

    (

     (substring(option agent.remote-id,0,9)="SPSI-AI00") and

     (substring(option agent.circuit-id,2,2)="\x02\x58")

    )

    or

    (

     (substring(option agent.remote-id,0,9)="SPSI-AI00") and

     (substring(option agent.circuit-id,3,2)="\x02\x58")

    )

  );

        set circuit-id = concat(option agent.circuit-id,"@",option agent.remote-id);

        spawn with pick(option agent.circuit-id, circuit-id);
        lease limit 5;

        log(info,concat("  EQUIP> ",option vendor-class-identifier, " is being used on Internet"));

}
```

31.2.2 spsi-ai00-awplus-class

```
# spsi-ai00-awplus-class for Service Provider Solutions Interop (SPSI) lab Access Island 0,
#   AlliedWare Plus access ports for provisioning 3play iMGs
# Jul-7-10 JWS: copied from spsi-ai00-class, modified for AW+
# Jul-23-10 JWS: changed for aw+ dhcp snooping
# Apr-3-12 JWS: added img1505

###############################################################################

# AGENT REMOTE ID:

# None, since not supported by AW+ 5.3.3-0.4

# AGENT CIRCUIT ID:

# Vlan 201 (RGBoot)     = vlan201      = 10.52.110.176    255.255.255.240

# Vlan 301 (RGMgmt)     = vlan301      = 10.52.110.192    255.255.255.240

# Vlan 401 (Voice)      = vlan401      = 10.52.110.208    255.255.255.240

# Vlan 501 (Video)      = vlan501      = 10.52.110.224    255.255.255.240

# Vlan 601 (Internet)   = vlan601      = 10.52.110.240    255.255.252.240

###############################################################################

### RG Boot vlan 201 ###

class "SPSI-AI00-AWPLUS-iMG646MODBoot" {
  match if ((option agent.circuit-id="vlan201") or (substring(option agent.circuit-id,2,2)="\x00\xc9"))
    and (option vendor-class-identifier = "iMG646MOD");
  filename "FIBER/AWPLUS/IMG646MOD";
  option tftp-server-name "10.52.201.4";
  option vendor-class-identifier "iMG646MOD";
}

class "SPSI-AI00-AWPLUS-iMG746MODBoot" {
  match if (option agent.circuit-id="vlan201") and (option vendor-class-identifier = "iMG746MOD");
  filename "FIBER/AWPLUS/IMG746MOD";
  option tftp-server-name "10.52.201.4";
  option vendor-class-identifier "iMG746MOD";
}

class "SPSI-AI00-AWPLUS-iMG1505Boot" {
  match if (option agent.circuit-id="vlan201") and (option vendor-class-identifier = "iMG1505");
  filename "FIBER/AWPLUS/IMG1505";
  option tftp-server-name "10.52.201.4";
  option vendor-class-identifier "iMG1505";
}

### RG Mgmt vlan 301 ###

class "SPSI-AI00-AWPLUS-iMG646MODMgmt" {
  match if ((option agent.circuit-id="vlan301") or (substring(option agent.circuit-id,2,2)="\x01\x2d"))
    and (option vendor-class-identifier = "iMG646MOD");
  option vendor-class-identifier "iMG646MOD";
# For TFTP discovery method
# option bootfile-name "10.52.201.4";
}

class "SPSI-AI00-AWPLUS-iMG746MODMgmt" {
  match if (option agent.circuit-id="vlan301") and (option vendor-class-identifier = "iMG746MOD");
  option vendor-class-identifier "iMG746MOD";
}

class "SPSI-AI00-AWPLUS-iMG1505Mgmt" {
  match if (option agent.circuit-id="vlan301") and (option vendor-class-identifier = "iMG1505");
  option vendor-class-identifier "iMG1505";
}

### RG VoIP vlan 401 ###

class "SPSI-AI00-AWPLUS-VoIP" {
  match if ((option agent.circuit-id="vlan401") or (substring(option agent.circuit-id,2,2)="\x01\x91"))
      and ((option vendor-class-identifier = "iMG646MOD")
        or (option vendor-class-identifier = "iMG746MOD"));
}


### Internet vlan 601 ###
```

```
class "SPSI-AI00-AWPLUS-Internet" {
  match if ((option agent.circuit-id="vlan601") or (substring(option agent.circuit-id,2,2)="\x02\x59"));
}
```

31.2.3 spsi-ai00-subnet

```
# spsi-ai00-subnet for Service Provider Solutions Interop (SPSI) lab Access Island 0
# Jul-15-08 JWS: modified for migration of nms server ip from 10.52.110.4 to 10.52.201.4
# Aug-11-08 JWS: modified for migration of dns domain from stelar.net to spsi.lab.telesyn.corp
# Feb-12-09 JWS: modified to add iMG613RF, iMG616BD
# Feb-13-09 JWS: modified to add iMG606BD
# Mar-31-09 JWS: modified to add iMG726MOD, iMG746MOD
# Jul-22-09 JWS: modified to add iMG616W
# Aug-7-09 JWS: modified to add domain server option in inet pool
# Oct-9-09 JWS: modified for iMG624A-R2
# Oct-22-09 JWS: modified for Comtrend NexusLink 5631 ADSL bonded CPE
# Feb-12-10 JWS: modified to completely add iMG634WA
# Sep-14-10 JWS: added dns options to rgboot, rgmgmt
# Apr-7-11 JWS: added iMG726BD-ON
# May-4-11 JWS: added iMG606BD-R2
# May-19-11 JWS: added iMG616BD-R2
# Aug-1-11 JWS: added iMG2504
# Aug-4-11 JWS: added iMG1525
# Oct-6-11 JWS: added iMG1505
# Dec-2-11 JWS: added iMG2524

################################################################################

# AGENT REMOTE ID:

# SPSI-AI00  (TEST [AI00] ACCESS ISLAND)  #

# AGENT CIRCUIT ID:

# Vlan 100 (MAPMgmt)    = \x00\x64      = 10.52.110.16   255.255.255.240 nonUFO

# Vlan 200 (RGBoot)    = \x00\xc8      = 10.52.111.0    255.255.255.192 UFO

# Vlan 300 (RGMgmt)     = \x01\x2c      = 10.52.111.64   255.255.255.192 UFO

# Vlan 400 (Voice)      = \x01\x90      = 10.52.111.128  255.255.255.192 UFO

# Vlan 500 (Video)      = \x01\xf4      = 10.52.111.192  255.255.255.192 UFO

# Vlan 600 (Internet)   = \x02\x58      = 10.52.110.64   255.255.252.224 UFO?

################################################################################


shared-network SPSI-AI00 {

  # MAPMgmt vlan subnet (/28 = 27 MAP devices)

  subnet 10.52.110.16 netmask 255.255.255.240 {

  }


  # RG/iMG voice vlan subnet (/26 = ~60 subscriber voice RG/iMG devices)

  subnet 10.52.111.128 netmask 255.255.255.192 {

    authoritative;

    ddns-updates on;

    ddns-update-style interim;

    ddns-domainname "rgvoip.spsi.lab.telesyn.corp";

    allow client-updates;

# start change JWS 2-Oct-07
# Changed ddns-ttl from 24h to 5m to workaround failure to ping new rgvoip ddns name
# after failed nms provisioning of img.
#    ddns-ttl 86400;
    ddns-ttl 300;

    ddns-rev-domainname "in-addr.arpa.";

    include "/etc/rndc.key";

    zone rgvoip.spsi.lab.telesyn.corp. {

       primary 10.52.201.36;
```

```
      key rndckey;
    }
    zone 111.52.10.in-addr.arpa. {
      primary 10.52.201.36;
      key rndckey;
    }
    pool {
      authoritative;
      range 10.52.111.132 10.52.111.190;
#       default-lease-time 86400;
      default-lease-time 300;
#       max-lease-time 86400;
      max-lease-time 300;
      option routers 10.52.111.129;
      option subnet-mask 255.255.255.192;
      option broadcast-address 10.52.111.191;
      option domain-name "rgvoip.spsi.lab.telesyn.corp";
      option domain-name-servers 10.52.201.36;
      option host-name = concat ("rgvoip-",(binary-to-ascii(16,8,"-",substring(hardware,1,6))));
      ddns-hostname = concat ("rgvoip-",(binary-to-ascii(16,8,"-",substring(hardware,1,6))));
      allow members of "SPSI-AI00-VoIP";
    }
  }

  # RG/iMG bootstrap vlan subnet
  subnet 10.52.111.0 netmask 255.255.255.192 {
    pool {
      authoritative;
      range 10.52.111.4 10.52.111.62;
      default-lease-time 600;
      max-lease-time 600;
      option routers 10.52.111.1;
      option subnet-mask 255.255.255.192;
      option broadcast-address 10.52.111.63;
      option domain-name "spsi.lab.telesyn.corp";
      option domain-name-servers 10.52.201.36;
      allow members of "SPSI-AI00-iBG915FXBoot";
      allow members of "SPSI-AI00-iMG613RFBoot";
      allow members of "SPSI-AI00-iMG606BDBoot";
      allow members of "SPSI-AI00-iMG606BD-R2Boot";
      allow members of "SPSI-AI00-iMG616BDBoot";
      allow members of "SPSI-AI00-iMG616BD-R2Boot";
      allow members of "SPSI-AI00-iMG616WBoot";
      allow members of "SPSI-AI00-iMG646BDBoot";
      allow members of "SPSI-AI00-iMG646BD-ONBoot";
      allow members of "SPSI-AI00-iMG646PX-ONBoot";
      allow members of "SPSI-A100-iMG626MODBoot";
      allow members of "SPSI-A100-iMG646MODBoot";
      allow members of "SPSI-A100-iMG726BD-ONBoot";
      allow members of "SPSI-A100-iMG726MODBoot";
      allow members of "SPSI-A100-iMG746MODBoot";
      allow members of "SPSI-A100-iMG1505Boot";
      allow members of "SPSI-A100-iMG1525Boot";
      allow members of "SPSI-A100-iMG2504Boot";
      allow members of "SPSI-A100-iMG2524Boot";
      allow members of "SPSI-A100-iMG634WABoot";
      allow members of "SPSI-A100-iMG624ABoot";
      allow members of "SPSI-A100-iMG624A-R2Boot";
      allow members of "SPSI-A100-iMG634ABoot";
      allow members of "SPSI-A100-iMG634A-R2Boot";
      allow members of "SPSI-A100-RG634ABoot";
      allow members of "SPSI-A100-RG624ABoot";
      allow members of "SPSI-A100-RG613TXBoot";
    }
  }

  # RG/iMG Remote Management vlan subnet
  subnet 10.52.111.64 netmask 255.255.255.192 {
    pool {
      authoritative;
      range 10.52.111.68 10.52.111.126;
      default-lease-time 86400;
      max-lease-time 86400;
      option routers 10.52.111.65;
      option subnet-mask 255.255.255.192;
      option broadcast-address 10.52.111.127;
      option domain-name "spsi.lab.telesyn.corp";
      option domain-name-servers 10.52.201.36;
      allow members of "SPSI-A100-iBG915FXMgmt";
      allow members of "SPSI-A100-iMG606BDMgmt";
      allow members of "SPSI-A100-iMG606BD-R2Mgmt";
      allow members of "SPSI-A100-iMG613RFMgmt";
      allow members of "SPSI-A100-iMG616BDMgmt";
      allow members of "SPSI-A100-iMG616BD-R2Mgmt";
      allow members of "SPSI-A100-iMG616WMgmt";
      allow members of "SPSI-A100-iMG646BDMgmt";
      allow members of "SPSI-A100-iMG646BD-ONMgmt";
      allow members of "SPSI-A100-iMG646PX-ONMgmt";
      allow members of "SPSI-A100-iMG626MODMgmt";
      allow members of "SPSI-A100-iMG646MODMgmt";
      allow members of "SPSI-A100-iMG726BD-ONMgmt";
```

```
      allow members of "SPSI-A100-iMG726MODMgmt";
      allow members of "SPSI-A100-iMG746MODMgmt";
      allow members of "SPSI-A100-iMG1505Mgmt";
      allow members of "SPSI-A100-iMG1525Mgmt";
      allow members of "SPSI-A100-iMG2504Mgmt";
      allow members of "SPSI-A100-iMG2524Mgmt";
      allow members of "SPSI-A100-iMG624AMgmt";
      allow members of "SPSI-A100-iMG624A-R2Mgmt";
      allow members of "SPSI-A100-iMG634AMgmt";
      allow members of "SPSI-A100-iMG634A-R2Mgmt";
      allow members of "SPSI-A100-iMG634WAMgmt";
      allow members of "SPSI-A100-RG634AMgmt";
      allow members of "SPSI-A100-RG624AMgmt";
      allow members of "SPSI-A100-RG613TXMgmt";
      allow members of "SPSI-A100-ComtrendMgmt";
    }
  }

  # RG/iMG Internet & PC vlan subnet
  subnet 10.52.110.64 netmask 255.255.255.224 {
    pool {
      authoritative;
      range 10.52.110.68 10.52.110.94;
      default-lease-time 1200;
      min-lease-time 1200;
      max-lease-time 3600;
      option routers 10.52.110.65;
      option subnet-mask 255.255.255.224;
      option broadcast-address 10.52.110.95;
      option domain-name-servers 10.52.201.36;
      allow members of "SPSI-A100-Internet";
    }
  }

 # STB Video vlan subnet
  subnet 10.52.111.192 netmask 255.255.255.192 {
    pool {
      authoritative;
      range 10.52.111.196 10.52.111.254;
      default-lease-time 86400;
      max-lease-time 86400;
      option routers 10.52.111.193;
      option subnet-mask 255.255.255.192;
      option broadcast-address 10.52.111.255;
      allow members of "aminet";
      allow members of "thomson";

      allow members of "SPSI-AI00-Video";

    }

  }

}
```

31.2.4 spsi-ai00-awplus-subnet

```
# spsi-ai00-awplus-subnet for Service Provider Solutions Interop (SPSI) lab Access Island 0,
#   AlliedWare Plus access ports for provisioning 3play iMGs
# Jul-7-08 JWS: copied from spsi-ai00-subnet, modified for AW+
# Apr-3-12 JWS: added img1505

##############################################################################

# AGENT REMOTE ID:

# None, since not supported by AW+ 5.3.3-0.4

# AGENT CIRCUIT ID:

# Vlan 201 (RGBoot)     = vlan201      = 10.52.110.176    255.255.255.240

# Vlan 301 (RGMgmt)     = vlan301      = 10.52.110.192    255.255.255.240

# Vlan 401 (Voice)      = vlan401      = 10.52.110.208    255.255.255.240

# Vlan 501 (Video)      = vlan501      = 10.52.110.224    255.255.255.240

# Vlan 601 (Internet)   = vlan601      = 10.52.110.240    255.255.252.240

##############################################################################

shared-network SPSI-AI00 {

  # RG/iMG bootstrap vlan subnet

  subnet 10.52.110.176 netmask 255.255.255.240 {
    pool {
      authoritative;
      range 10.52.110.178 10.52.110.190;
      default-lease-time 600;
      max-lease-time 600;
      option routers 10.52.110.177;
      option subnet-mask 255.255.255.240;
      option broadcast-address 10.52.110.191;
      allow members of "SPSI-AI00-AWPLUS-iMG646MODBoot";
      allow members of "SPSI-AI00-AWPLUS-iMG746MODBoot";
      allow members of "SPSI-AI00-AWPLUS-iMG1505Boot";
    }
  }


  # RG/iMG Remote Management vlan subnet

  subnet 10.52.110.192 netmask 255.255.255.240 {
    pool {
      authoritative;
      range 10.52.110.194 10.52.110.206;
      default-lease-time 86400;
      max-lease-time 86400;
      option routers 10.52.110.193;
      option subnet-mask 255.255.255.240;
      option broadcast-address 10.52.110.207;
      option domain-name-servers 10.52.201.36;
      allow members of "SPSI-AI00-AWPLUS-iMG646MODMgmt";
      allow members of "SPSI-AI00-AWPLUS-iMG746MODMgmt";
      allow members of "SPSI-AI00-AWPLUS-iMG1505Mgmt";
    }
  }


  # RG/iMG Internet & PC vlan subnet

  subnet 10.52.110.240 netmask 255.255.255.240 {
    pool {
      authoritative;
      range 10.52.110.242 10.52.110.254;
      default-lease-time 1200;
      min-lease-time 1200;
      max-lease-time 3600;
      option routers 10.52.110.241;
      option subnet-mask 255.255.255.240;
      option broadcast-address 10.52.110.255;
      option domain-name-servers 10.52.201.36;
      allow members of "SPSI-AI00-AWPLUS-Internet";
    }
  }


 # STB Video vlan subnet

  subnet 10.52.110.224 netmask 255.255.255.240 {
    pool {
      authoritative;
      range 10.52.110.226 10.52.110.238;
      default-lease-time 86400;
      max-lease-time 86400;
      option routers 10.52.110.225;
      option subnet-mask 255.255.255.240;
      option broadcast-address 10.52.110.239;
      allow members of "aminet";
      allow members of "thomson";
    }
  }
}
```

31.3 DNS Configuration File

```
        options {
        allow-transfer { 10.3.0.5; };
        directory "/etc/named.d/";
        /* 10.3.0.5 is the redundant DNS (slave)
         * 10.4.0.5 is the primary DNS
         * 10.3.0.2 and 166.163.128.5 are two DHCP servers
         * If there is a firewall between you and nameservers you want
         * to talk to, you might need to uncomment the query-source
         * directive below.  Previous versions of BIND always asked
         * questions using port 53, but BIND 8.1 uses an unprivileged
         * port by default.
         */
        // query-source address * port 53;
        };


# Use with the following in named.conf, adjusting the allow list as needed:
 key "rndc-key" {
       algorithm hmac-md5;
       secret "VBd+VWbItNu5ZtKJbRKgqQ==";
       };
 controls {
       inet 0.0.0.0 port 953
       allow {127.0.0.1;} keys{"rndc-key";};
       };

acl dhcp-srvr {10.3.0.2;166.163.128.5 ;

logging {
        channel normal_logs {
                severity info;                  // level 3 debugging to file
                file "/var/log/named";           // /var/adm/named
                print-time yes;                 // timestamp log entries
                print-category yes;              // print category name
                print-severity yes;             // print severity level
       };

        category default \{ normal_logs; };
       };

/**/
/*DDNS STUFF*/
/**/

/*VOICE REVERSE LOOKUP DDNS*/
zone "0.48.10.in-addr.arpa." {
        type master;
        allow-update { dhcp-srvr; };
        file "ddns/10.48.0.ndb";
        };


zone 1.85.10/.in-addr.arpa." {
        type master;
        allow-update { dhcp-srvr; };
        file "ddns/10.85.1.ndb";
        };


zone "1.48.10.in-addr.arpa." {
        type master;
        allow-update { dhcp-srvr; };
        file "ddns/10.48.1.ndb";
        };
```

```
zone "2.48.10.in-addr.arpa." {
        type master;
        allow-update { dhcp-srvr; };
        file "ddns/10.48.2.ndb";
        };
zone "3.48.10.in-addr.arpa." {
        type master;
        allow-update { dhcp-srvr; };
        file "ddns/10.48.3.ndb";
        };

zone "4.48.10.in-addr.arpa." {
        type master;
        allow-update { dhcp-srvr; };
        file "ddns/10.48.4.ndb";
        };


zone "5.48.10.in-addr.arpa." {
        type master;
        allow-update { dhcp-srvr; };
        file "ddns/10.48.5.ndb";
        };


zone "6.48.10.in-addr.arpa." {
        type master;
        allow-update { dhcp-srvr; };
        file "ddns/10.48.6.ndb";
        };


zone "7.48.10.in-addr.arpa." {
        type master;
        allow-update { dhcp-srvr; };
        file "ddns/10.48.7.ndb";
        };



/*RG FORWARD LOOKUP DDNS*/
zone "rg" {
        type master;
        allow-update { dhcp-srvr; };
        file "ddns/rg.ndb";
        };

/**/
/*END OF DDNS*/
/**/

/*Fixed REVERSE LOOKUP DNS files here...*/
zone "2.1.10.in-addr.arpa." {
        type master;
        file "networks/10.1.2.ndb";
        };

zone "3.1.10.in-addr.arpa." {
        type master;
        file "networks/10.1.3.ndb";
        };

zone "4.1.10.in-addr.arpa." {
        type master;
        file "networks/10.1.4.ndb";
        };

zone "5.1.10.in-addr.arpa." {
        type master;
        file "networks/10.1.5.ndb";
        };

zone "6.1.10.in-addr.arpa." {
        type master;
        file "networks/10.1.6.ndb";
        };


zone "0.3.10.in-addr.arpa." {
        type master;
        file "networks/10.3.0.ndb";
        };


zone "0.4.10.in-addr.arpa." {
        type master;
        file "networks/10.4.0.ndb";
        };
```

```
zone "1.6.10.in-addr.arpa." {
        type master;
        file "networks/10.6.1.ndb";
        };

zone "2.6.10.in-addr.arpa." {
        type master;
        file "networks/10.6.2.ndb";
        };

zone "1.40.10.in-addr.arpa." {
        type master;
        file "networks/10.40.1.ndb";
        };

zone "map" {
        type master;
        file "master/map.ndb";
        };

zone "net" {
        type master;
        file "master/net.ndb";
        };
```

32. Northbound Interface

A northbound interface on an NMS/EMS allows other software applications (higher level network management systems) to communicate with (or manage) the lower level NMS without the user acting on the lower level NMS directly. In many cases this interface is intended for higher level network management systems communicating with devices from different vendors (with vendor specific device communication interfaces) using element management systems from those vendors that provide a well known interface that can be used by the higher level network management software.

There are several platform-independent technologies of software communication used to implement the northbound interface (e.g. CORBA, XML, RMI, etc.) and Apache Axis will be used to provide the northbound interface in Allied*View* NMS. Axis is an implementation of SOAP (Simple Object Access Protocol) which is not only XML based but also provides APIs that support web services standards.

The following table lists the capabilities for the northbound interface APIs.

TABLE 32-1 Northbound Interface APIs

Capability	Detail
Retrieve network inventory objects from NMS based on criteria set by the client.	Provide APIs for retrieving network inventory data based on type and allow client application to specify other criteria. In addition the API will allow clients to retrieve any other network inventory data from the NMS by specifying the matching criteria.
Retrieve network events available in NMS database based on criteria set by the client.	Allow clients to retrieve network events from the NMS. The client can specify criteria of the network events to be retrieved. Only events that match the selected criteria will be retrieved.
Retrieve alarms available in NMS database based on criteria set by the client.	Allow clients to retrieve alarms from the NMS. The client can specify criteria of the alarms to be retrieved. Only alarms that match the selected criteria will be retrieved.
Retrieve network events and alert filters that are currently configured in NMS.	Allow clients to retrieve all event and alert filters configured in NMS. These filters in NMS could be setup to perform certain operations when a new event or alert is received.
Retrieve trap and events parsers that are currently configured in NMS.	Allow clients to retrieve all trap and event parsers configured in NMS. These parsers in NMS are used to modify any properties of the trap or event in NMS (by default these are used to set the severity)
Retrieve the number of network events or alarms in the NMS.	Allow clients to retrieve total counts for all events and alarms from the NMS. Alarm counts can also be retrieved for the specified severity.
Retrieve the history of an alarm	The NMS maintains the history of an alarm based on failure object (entity) which will be available through this API. The client will specify the failure object of the alert to get the history.
Autonomous events configuration for clients	allow clients to receive network events from the NMS immediately without the need for the client to poll the NMS every time. The client will configure the NMS with the information required (including criteria if only specific events are needed) and the NMS will forward all events that match the criteria

TABLE 32-1 Northbound Interface APIs

Capability	Detail
Retrieve device information from the device through the NMS	All other operations in this release operate on the NMS with the results available in the NMS server. This operation will use the NMS to retrieve the data from the device. Device data is retrieved using CLI or SNMP. The main purpose for this is to evaluate how other device operations can be supported
Users accessing northbound interface must be authenticated and denied access if not authorized.	Operations done through the northbound interface will have access to the NMS database and devices, therefore access should be restricted using the users in NMS security database
Retrieve stored customer information from device	Once the configuration is complete the northbound interface is expected to have an API to retrieve the configured information from the device. This can be used to allow clients to validate parameters or display subscribed services.
Provision a triple play customer.	Allows northbound interface clients to provision triple play services for a customer using iMAP device and RG or iMG device.
Provision a customer port on device	Allows northbound interface clients to provision a customer port on iMAP device without provisioning the RG or iMG device.
Provision a customer RG or iMG device	Allows northbound interface clients to provision services on the RG for a customer when the port where the RG is connected was provisioned separately.
De-provision a triple play customer.	Allows northbound interface clients to de-provision triple play services for a customer on iMAP device and RG or iMG device through the API. The iMAP port and RG can also be de-provisioned separately.
Modify Customer provision information.	Allows northbound interface clients to modify selected provision information for the customer. Configuration information that can be modified is similar to what was used in provisioning.
Perform a bulk provision task (provision many customers from saved data)	Allows provision, de-provision or modify configuration of many customers by loading the information from a file. The client in NMS that has limited bulk provision operations is currently using RMI and is updated to use northbound operations.

32.1 SOAP Implementation

32.1.1 Apache Axis

Apache Axis is able to provide web services, and as a successor of SOAP, it has the simplicity for hiding all XML details from the users implementing the service or clients. Administrators can find detailed information on Axis/SOAP at www.apache.org.

Note: *Apache Axis is described here because the AlliedView NMS server implementation is based on Apache Axis for SOAP communication. Other web service tools besides Axis could be used.*

Note: *Axis 1 (1.4) does not support callback operations and is considered slower compared to other technologies such as CORBA because it uses HTTP as the protocol and text (XML) data. Axis 2 (currently in beta version) is expected to be an improvement of its predecessor.*

Note: *With a standard northbound interface, the higher level NMS would not have to implement different clients to communicate with NMS/EMS from different vendors. However, specific interfaces may be more useful to the client because operations will be specific to clients' needs.*

32.1.2 WSDL

WSDL is a language used to describe the services published by an interface. When publishing Axis web services, the server will include interfaces and implementations and publish the WSDL file which will include descriptions of all available operations, parameters and return types.

Note: *The WSDL in Axis/SOAP is considered equivalent of the IDL in CORBA.*

On the client side the implementation can start by looking at the WSDL file to determine available services, generate stub code from WSDL then implement the client to use the services. As an alternative client implementation can skip client code generation and manually implement client code that calls Axis directly (this can be complicated if the developer is not familiar with Axis/SOAP core classes). There are tools already available that can be used to parse WSDL files and generate stubs and skeleton code for different language implementations.

For the WSDL path for AlliedView NMS, use http://<nmsserver-IP>:9090/axis/services

Client programs intended for performing operations on NMS using this interface can be implemented in any language that supports SOAP; however languages that do not support HashMaps will be limited to operations that do not take a HashMap as a parameter or return it as results. The WSDL file provided contains all operations available and the client program developer will need to use it to get the correct syntax of operations and details provided here will be useful explaining object contents.

32.1.3 Web Services

Web services are essentially application interfaces available for communication with other programs that can be done through the web (HTTP server). The northbound interface in NMS will be available through the web server and can be executed from anywhere if the server is accessible from the internet. The APIs and features exposed will also be referred to as web services.

The following figure shows how Axis/Soap clients fit into the client/server model. Among other processes running in the NMS server are the web server and servlet container which are used to service Axis requests. Axis/SOAP client communicates with the web server which forwards the request to Tomcat container and returns the results for the operation from the container to the Axis client. Other clients also use Apache and Tomcat i.e. Java clients use HTTP server and servlets to launch WebStart and Applet clients and HTML clients use the HTTP server for HTML pages and Tomcat container to process JSP requests.

Axis/SOAP transports data using XML sent over HTTP. SOAP converts the client requests to XML and sends it to the HTTP server, which forwards the request to Tomcat container. The response is also converted to XML from the container before returned to client and the client converts it back from XML to objects expected by the client

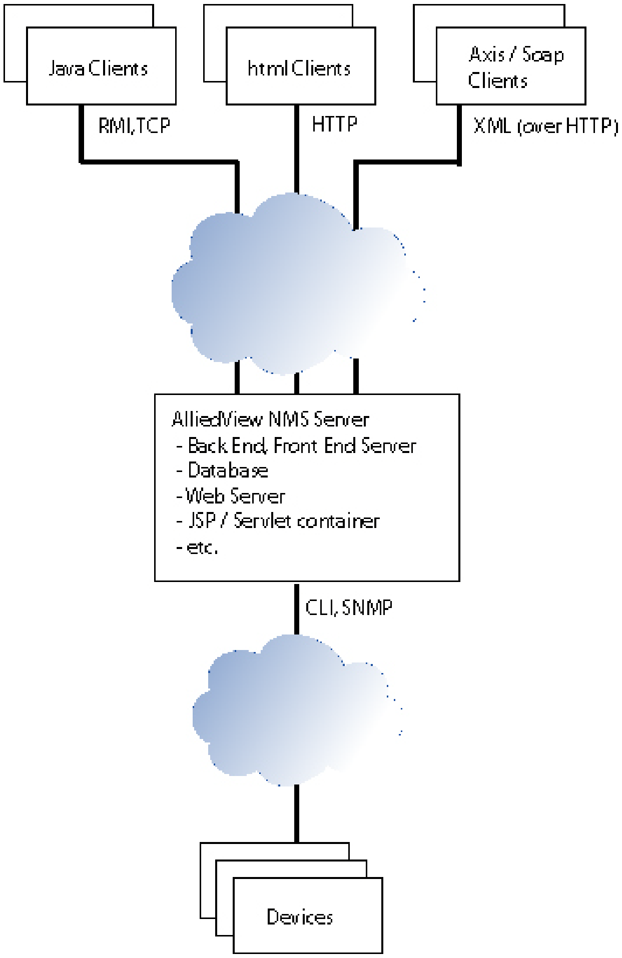


FIGURE 32-1 Client / Server Model for AlliedView NMS

32.2 User Interaction

32.2.1 Web Services Activation

Web services in NMS will not be activated by default and can be activated at runtime when needed by the NMS administrator. When not in use the administrator can also deactivate web services provided by NMS. The script AT_WebService.bat/sh can be used to enable and disable the APIs when executed as below. Note that restarting the server is not required when activating/deactivating NMS web services APIs and the server must be running when performing these tasks.

32.2.1.1 Activate Web Services (Axis/SOAP)

This operation must be done after the server is started.

1. Change directories to <NMS_HOME>/bin
2. Execute AT_WebService.bat/sh with ‘deploy’ parameter
    - AT_WebService.bat deploy (Windows)
    - AT_WebService.sh deploy (Linux)

32.2.1.2 Review the Associated WSDL and Available Services

Use http://<nmsserver-IP>:9090/axis/services to see the WSDL and the services available. Note that a relevant file is available only after activating the web services.

32.2.1.3 Deactivate Web Services (Axis/SOAP)

This operation must be done after the server is started.

1. Change directories to <NMS_HOME>/bin
2. Execute AT_WebService.bat/sh with 'undeploy' parameter
   - AT_WebService.bat undeploy (Windows)
   - AT_WebService.sh undeploy (Linux)

32.2.2 User Security

Security will use existing security concepts, which requires a correct user and password and the user must be authorized to perform the requested operation. Audit trails will be logged only in operations that make modification to NMS or devices (e.g. setEventTarget and removeEventTarget in this release).

In NMS there are several operations that are not restricted to any user and the default behavior will be used for their corresponding web service operation. All northbound APIs that have corresponding operations already in NMS will use the security restrictions for those operations. If the user could not be authenticated (invalid user and/or password) or if not authorized to perform the requested operation, the operation fails and the client will get an AxisFault exception with the failure reason.

32.2.3 Operation Threshold Activation

The administrator can set the threshold that allows the specified number of operations to be executed over a specific time interval. This is intended to reduce the server load from processing excessive number of operations and affecting other services. This should be done after the administrator and those implementing clients for this interface decide on what thresholds are acceptable based on the NMS server usage. When thresholds are exceeded the next operations will be denied and stricter restrictions will be enforced until operation execution rate is reduced to current restriction before returning to normal execution rate. By default this feature is not activated and all web service operations will be processed normally.

32.2.3.1 Activate

Create (or edit) a file NMS_HOME/conf/AT_tmp_conf.properties and specify the properties, then restart the NMS server:

- WS_PROCESS_COUNT=<number> - (for operations count)
- WS_INTERVAL=<number> - (for time interval in seconds)

32.2.3.2 Deactivate

To deactivate, comment out the entries in the file above by using the # character in the beginning of the line (or delete the file if those are the only two entries), then restart the server

32.2.4 Axis/SOAP Interface Client Development - Examples

Client programs intended for performing operations on NMS using this interface can be implemented in any language that supports SOAP; however languages that do not support HashMaps will be limited to operations that do not take a HashMap as a parameter or return it as results. The WSDL file provided contains all operations available and the client program developer will need to use it to get the correct syntax of operations and details provided here will be useful explaining object contents.

32.2.4.1 Client Implementation

There are several ways to implement a client program and several tools are also available to simplify web services development. Here are some examples:

- Use the WSDL provided with client code generator tools (e.g. wsdl2java, wsdl2cpp, etc.) to generate client stub source code for the client to use when calling remote objects. (faster and easier to follow)
- Use an IDE software packages that read the WSDL and guide the client development based on the available interface. (can be slow for experienced programmers)
- Develop the client that manually calls SOAP classes and pass all operation and parameters for the operation. (Requires more SOAP understanding and good if you need to access the SOAP message properties directly.)

32.2.4.2 Example Class (Java)

This example will use Java but other languages have a similar mechanism to generate stub source code and here the example will use Inventory module in NMS

1. Activate the available web services in NMS (refer to "Activate Web Services (Axis/SOAP)" on page 1120).
2. Point the browser to web services URL path on NMS server to see the deployed services and get the Inventory WSDL contents into a file (Inventory.wsdl).
3. Run the wsdl2java tool with Inventory.wsdl (See Java or Axis/SOAP documentation) to generate stubs (you will then have at least InventoryService, InventorySoapBindingStub and InventoryInterface classes).
4. The generated classes have all the information needed to access the NMS web service Write the client code to use the generated classes (see example below) with the correct parameters.
5. Compile your class together with the generated classes and run your code that calls web services.

32.2.4.3 Accessing Examples

A complete set of examples is included with release 10.0 in the <NMS_home>/examples directory. There is the nb_examples.zip file, which when extracted contains a set of guidelines and examples. Open the readme text file first.

32.2.5 Available Operations

There are many operations available through northbound interface in NMS with different parameter and results types. The WSDL defines the syntax of all parameters and results but does not define what is the 'Object' included in Lists (object arrays) or HashMaps which have different values based on operation. However, when used in parameters generally Lists will contain a collection of string objects and HashMaps will contain key/value pairs which are both string objects.

Many of the operations that take a HashMap parameter as a filter criteria will accept a '*' anywhere in the string and a '!' at the beginning of the string with their respective meanings when matching the criteria.

The table below show details of available operations in release 9.0 and the key words listed here will be used in the table. Properties of objects used are as they are stored in NMS database or retrieved from device and multiple parameters are listed as they appear.

- MO match criteria: A HashMap of match criteria key/value pairs using Managed Object properties (e.g. category=Rapier, type=9700 etc.). Criteria can be left empty to match anything or use selected special characters mentioned above (some operations require match to specific devices).
- List of object properties: A list (array of objects) with each element containing properties of one object in a HashMap
- Provision properties: A map of parameters used in provisioning the device (see "Provision Parameters" on page 1125 for the list)

.

TABLE 32-2 Operations Table

Module / Operation	Parameters Types	Return Types	Notes
Inventory/ getNodeNames	*MO match criteria* (Nodes)	List of node names	Returns a list of node names matching the criteria
Inventory/ getNetworks	*MO match criteria* (Networks)	*List of object properties* (Networks)	Return a list of network object properties matching the criteria
Inventory/ getNodes	*MO match criteria* (Nodes)	*List of object properties* (Nodes)	Return a list of node object properties matching the criteria
Inventory/ getCards	*MO match criteria* (Cards)	*List of object properties* (Cards)	Return a list of node object properties matching the criteria
Inventory/ getPorts	*MO match criteria* (Ports)	*List of object properties* (Ports)	Return a list of port object properties matching the criteria
Inventory/ getIpInterfaces	*MO match criteria* (IP interfaces)	*List of object properties* (IP interface)	Return a list of IP interface object properties matching the criteria
Inventory/ getVlanInterfaces	*MO match criteria* (VLAN interfaces)	*List of object properties* (VLAN interfaces)	Return a list of VLAN interface object properties matching the criteria
Inventory/ getVlans	*MO match criteria* (VLANs)	*List of object properties* (VLANs)	Return a list of VLAN object properties matching the criteria
Inventory/ getPhysicalLinks	*MO match criteria* (Physical links)	*List of object properties* (Physical links)	Return a list of physical link object properties matching the criteria
Inventory/ getEpsrDomains	*MO match criteria* (EPSR domains)	*List of object properties* (EPSR domains)	Return a list of EPSR domain object properties matching the criteria
Inventory/ getProfiles	*MO match criteria* (Profiles)	*List of object properties* (Profiles)	Return a list of profile object properties matching the criteria
Inventory/ getTasks	*MO match criteria* (Tasks)	*List of object properties* (Tasks)	Return a list of task object properties matching the criteria
Inventory/ getInventoryObjects	*MO match criteria* (any MO objects types)	*List of object properties* (any objects types)	Return a list of any object properties matching the criteria
Inventory/ getDiscoveryProperties	None	HashMap of discovery properties	Returns discovery configuration properties
Faults/ getTotalEventsCount	None	Total events count (integer)	Returns total number of events
Faults/ getEvents	HashMap of event properties match criteria	List of event properties (list of HashMaps)	Returns a list of event properties matching the criteria

TABLE 32-2 Operations Table

Module / Operation	Parameters Types	Return Types	Notes
Faults/ getEventFilters	None	HashMap of event filters with each filter containing a HashMap that has criteria and actions. Criteria contain strings and an action contains a HashMap with different actions.	Returns a HashMap of event filters. This Map contains other HashMaps for criteria and actions and also actions contain other HashMaps for each action.
Faults/ getEventParsers	None	List of event parser properties (list of HashMaps)	Returns a list of event parsers properties
Faults/ getTrapParsers	None	List of trap parser properties (list of HashMaps)	Returns a list of trap filter properties
Faults/ setEventTarget	- Target server IP address - Target server port number - HashMap of event properties match criteria	None	Sets up a target server and port as a receiver of events that match the specified criteria.
Faults/ removeEventTarget	- Target server IP address - Target server port number	None	Remove the server with address and port from events receiver.
Faults/ getEventTargets	None	HashMap of event targets which also shows counts	Returns the configured event target hosts and ports.
Faults/ getTotalAlertsCount	None	Total alarms count (integer)	Returns total number of alarms
Faults/ getAlertsCount	Severity string (e.g. Critical, Major, etc.)	Alarms count with the severity.	Returns the number of alarms matching the specified severity
Faults/ getAlerts	HashMap of alarm properties match criteria	List of alarm properties (list of HashMaps)	Returns a list of alarm properties matching the criteria
Faults/ getAlertFilters	None	HashMap of alarm filters with each filter containing a HashMap that has criteria and actions. Criteria contain strings and an action contains a HashMap with different actions.	Returns a HashMap of alarm filters. This Map contains other HashMaps for criteria and actions and also actions contain other HashMaps for each action.
Faults/ getAlertAnnotation	Failure object (entity) of the alarm	List of annotation properties for the alarm (list of HashMaps)	Returns a list of annotations for the alarm with the specified entity.
Faults/ getAlertHistory	Failure object (entity) of the alarm	List of history properties for the alarm (list of HashMaps)	Returns a list of history for the alarm with the specified entity.

TABLE 32-2 Operations Table

Module / Operation	Parameters Types	Return Types	Notes
Mdti/ getDeviceInfo	Device IP address (a in NMS database)	HashMap or device general information properties	Returns device general information from the device. This retrieves results from the device (not database).
Mdti/ getMultiDeviceInfo	Device IP addresses (separated by ‘,’)	List of properties (list of HashMaps)	Returns a list of device general information properties
Provision/ getDeviceInterfaces	- Device IP address - Port number	A map of parameters of the interface specified	Returns current values from the device (if ALL is specified then values returned will be for all ports)
Provision/ getDeviceVlans	- Device IP address - VLAN ID	A map of properties of the specified VLAN	Returns current values from the device (if ALL is specified then values returned will be for all VLANs)
Provision/ getRGDeviceDetails	- MO match criteria (RGs) - Components list	Map containing properties of the RG	Retrieves properties of RG from the device directly.
Provision/ provisionPort	*Provision parameters*	Status of the operation	Status returned can indicate the operation has started or completed if time-out is specified.
Provision/ deprovisionPort	*Provision parameters*	Status of the operation	Status returned can indicate the operation has started or completed if time-out is specified.
Provision/ modifyPort	*Provision parameters*	Status of the operation.	Status returned can indicate the operation has started or completed if time-out is specified
Provision/ modifyRG	*- MO match criteria (RGs)* *- Provision parameters*	Status of the operation	Status returned can indicate the operation has started or completed if time-out is specified.

32.2.6 Provision Parameters

Most of the provision operations will use parameters grouped in key/value format (HashMap). Accepted keys are already specified and will need to be used as expected for the operation to be executed; unknown keys will be ignored. Most of these keys have values that are also specific but some will accept user specified values.

The table below contains keys and possible values that can be used with it. Keys selected use names that relate to where they are expected to be used. These parameters are very similar to those that are provisioning windows and used here to configure same parameters on devices. The order of these parameters as they appear in a map does not affect the execution of the operation and there are more than these included here.

TABLE 32-3 Provision Parameters

Keys	Values	Description
DEVICE	<IP address>	IP address of the iMAP device
SLOT_PORT	<Port number>	Slot and port number of the selected port (X.Y)
PORT_PROFILE	<Port profile name>	RG general profile name
RG_INET_PROFILE	<RG internet profile name>	RG internet profile name
RG_VIDEO_PROFILE	<RG video profile name>	RG video profile name
RG_VOIP_PROFILE	<RG VOIP profile name>	RG VOIP profile name
CUSTOMER_ID	<Customer ID>	Unique customer ID
CUSTOMER_INFO	<Customer info>	Any customer information
PORT_STATUS	(ENABLED/DISABLED)	Enable/Disable iMAP port
DHCP_AGEING	(ON/OFF)	Enable/Disable DHCP ageing on iMAP device
MAX_LEARNED_MAC_ADDRS	(OFF/1..64)	MAC address learn limit
IP_RANGES	<IP filter ranges>	Comma separated IP ranges
MAC_ADDRESSES	<Allowed MAC addresses>	Comma separated list of MAC addresses
TAGGED_VLANS	<Tagged VLANs>	Comma separated list of tagged VLANs for iMAP port
UNTAGGED_VLAN	<Untagged VLAN>	Untagged VLAN for iMAP port
TLS_VLAN	<TLS VLAN>	A VLAN for transparent LAN
PROVISION_DATA	(TRUE/FALSE)	Include iMAP port in provision
DEPROVISION_DATA	(TRUE/FALSE)	Include iMAP port in deprovision
PROVISION_RG	(TRUE/FALSE)	Include RG device in provision
DEPROVISION_RG	(TRUE/FALSE)	Include RG device in deprovision
RG_PROFILE_VLANS	(TRUE/FALSE)	Specify where to use VLANs from RG profiles specified
LOCAL_VLAN	<RG local VLAN>	RG VLAN for local network
LOCAL_IP	<RG local IP address>	RG local network address
LOCAL_MASK	<RG local netmask>	RG local network mask
DHCP_START_IP	<RG local DHCP start IP address>	RG local DHCP start IP address
DHCP_END_IP	<RG local DHCP end IP address>	RG local DHCP end IP address
INET_IP	<RG internet IP address>	RG IP address for internet service if not from DHCP
INET_MASK	<RG internet netmask>	RG netmask for internet service if not from DHCP
VOIP_IP	<RG VOIP IP address>	RG IP address for VOIP service if not from DHCP
VOIP_MASK	<RG VOIP netmask>	RG netmask for VOIP service if not from DHCP
RG_PORT_SERVICE_X	(INTERNET/VIDEO/TLS)	RG Ethernet port service (X is port number)

TABLE 32-3 Provision Parameters

Keys	Values	Description
RG_PORT_SPEED_X	(AUTO/COAX/ FULL_100M/HALF_100M/ FULL_10M/HALF_10M)	RG Ethernet port speed (X is port number)
RG_PORT_UP_RATE_X	<Port upstream rate>	RG Ethernet port upstream rate in kbps (X is port number)
RG_PORT_DOWN_RATE_X	<Port downstream rate>	RG Ethernet port downstream rate in kbps (X is port number)

33. Using the HTML Interface

Use the following table to locate the most common tasks you wish to perform. If you are using the NMS, use the screen name or the form name as well to locate the relevant section.

TABLE 33-1 Task List for HTML Interface

Task	Screen / Form Name (if Applicable)	Section/Notes
Change Password	Not applicable (n/a)	(Modifying the User Account and Password)
Review Screen	n/a	(Initial Screen Layout (Function Tabs))
Network Map Tasks		Overview (Network Maps)
Manage Alarms	Alarms	Review Screen (Overview of Alarms)
Manage Network Events	Network Events Event Details	Review Screen (Overview of Network Events) View Details (Viewing Event Details)
Managing Network Inventory	Network Inventory Object Details	Review Screen (Network Inventory) (Network Inventory View Options)
Managing Nodes	SNMP MIB Manager	Working with SNMP Tools (MIB Manager)
Setting up Users	n/a	Admin (User and Network)
Logging Out	Main screen, logout option	Note: If you log out by closing the browser, it requires 30 minutes for the client session to time out. Use the Logout option.

33.1 Starting Up

You can view the HTML interface through any web browser, such as Mozilla or Internet Explorer. Open the web browser and type the machine name and port number of the server in the address bar, as shown below:

```
http://<machine name>:<port number>
```

For example:

```
http://nms-server:9090
```

In the above example, nms-server is the name of the machine in which the server is running, and 9090 is the port number on which the server is listening.

Note: *The NMS HTML interface does not have all the features and functions of the Java interface, and is therefore more suitable for query and report functions that can be accessed over any compatible browser. There are administrative tasks that can be done, but these should be done by authorized personnel only.*

33.1.1 Setting Web Browser Caching

The web browser caching function should be set to always check for updates from the server before retrieving content from cache.

For example, with IE, use *Tools -> Internet Options* and click on the General tab. Under Temporary Internet files, select **Settings...**

In the **Settings** window, under **Check for newer versions of stored pages**:, select the button **Every visit to the page**.

33.1.2 Modifying the User Account and Password

There are several situations in which the user account status or password must be modified. These include:

- Setting up user names and passwords for the first time.
- The password has expired - If you try to log in to the NMS Server when your password has expired, you get a message stating that your password has expired.
- The user account has expired - If you try to log in to the AlliedView NMS Server when your user name has expired, you get the message:

  The User Account has EXPIRED. Please contact the Administrator.

  You will have to contact your NMS Administrator to have your account renewed.
- The user account has been disabled - If you try to log in to the AlliedView NMS Server when your user account is disabled, you get the message:

  The User Account has been DISABLED. Please contact the Administrator.

  You will have to contact your NMS Administrator to have your account re-enabled.

33.2 Common Interface Components

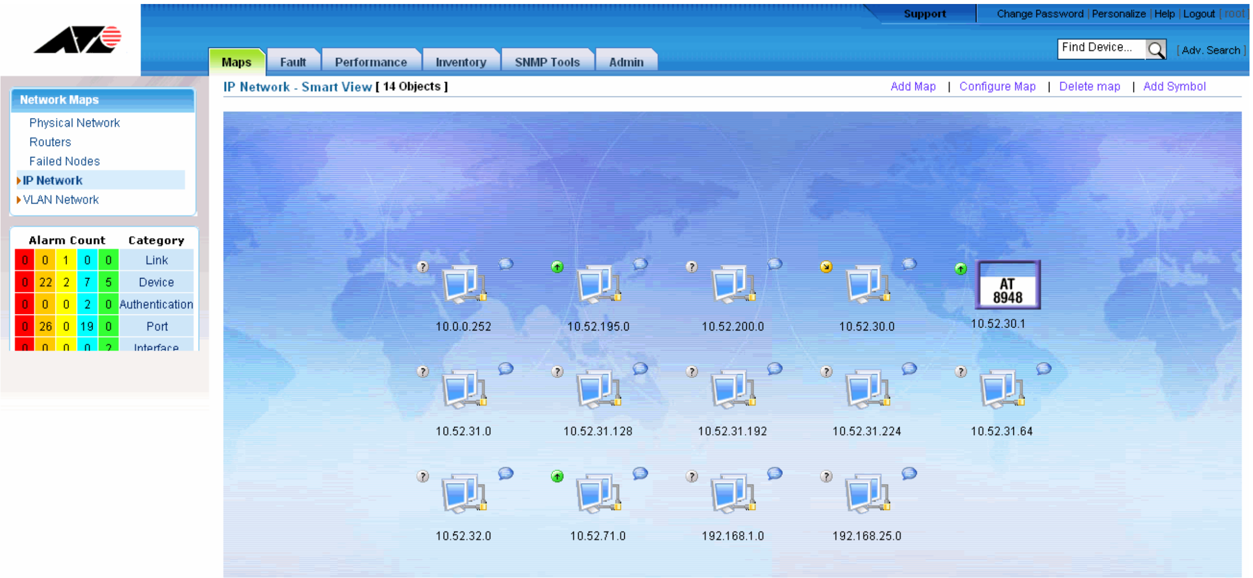
After you have logged into the browser HTML client by giving a valid user name and password, the screen displays the following three frames: the Tree frame, Display frame, and the Alarm Count frame. An example screen is shown in Figure 33-1. This section explains the various setups available initially on the screen.

33.2.1 Initial Screen Layout (Function Tabs)

The initial screen has the following components:

- At the top of the html frame is a set of function tabs. Each tab controls what appears in the Tree Frame and Display Frame. Directly underneath the tabs is a reminder of where the user is in the tab hierarchy.
- The **Tree Frame** is on the left-hand side of the screen. It has the tree that displays the different nodes for the chosen function tab.
- The **Alarm Count Frame** is on the left-bottom corner of the screen. It shows the categories of alarms, based on severity. Clicking on any number will list the associated alarms in the Alarm view. This frame appears regardless of which tab has been selected. The Alarm view is explained in Fault Management (Events and Alarms).
- The **Display Frame** is on the right side of the screen. It shows the different nodes or tables for the node chosen in the Tree frame.

Refer to the following figure for an example initial screen and what icons mean.



Alarm Count					Category
0	0	1	0	0	Link
0	22	2	7	5	Device
0	0	0	2	0	Authentication
0	26	0	19	0	Port
0	0	0	0	2	Interface

FIGURE 33-1 Initial Screen for html Interface

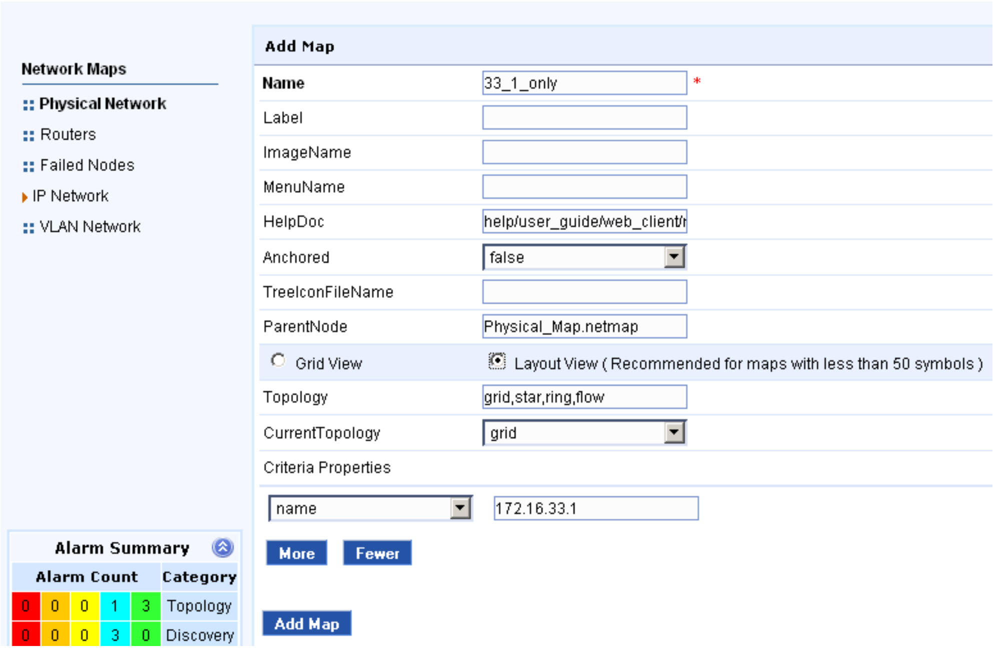
33.2.2 Search Function

To search for a particular device, the user can input a device attribute in the Find Device field, and then select GO. The Adv. Search brings up the Network Inventory View (explained later) with a Search Criteria options.

33.2.3 Maps and Symbols

For all the map types, the user has the following options:

- Add Map - This allows the user to add a map type to the Network Map tree. The newly created map will appear as a node of where the user is currently at; for example if the user is at the Physical Network Node and creates a map, the new map will appear as a node (leaf) under the Physical Network node. In the example below, the user has created a map called 33_1_only to show only a single device.



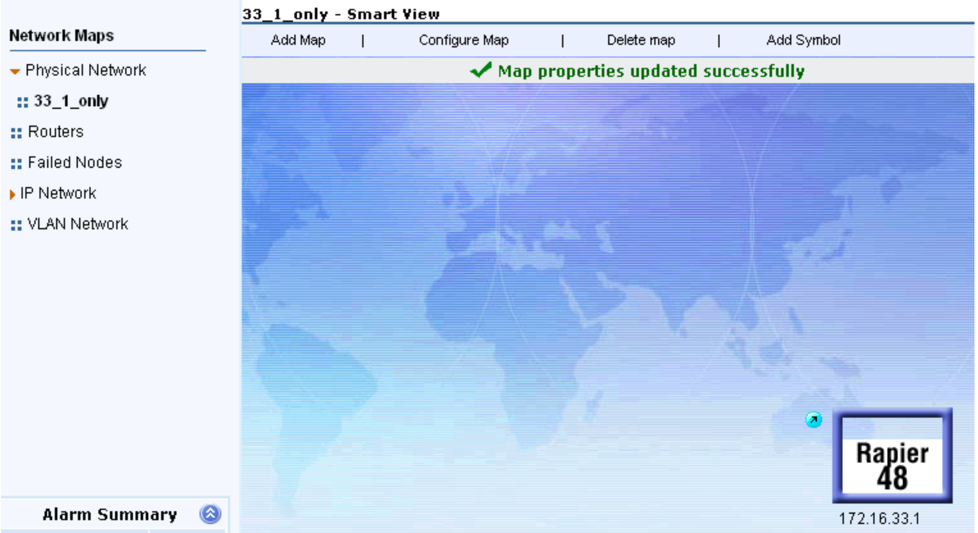
Add Map

Name	33_1_only *
Label	
ImageName	
MenuName	
HelpDoc	help/user_guide/web_client/r
Anchored	false
TreeIconFileName	
ParentNode	Physical_Map.netmap
○ Grid View	● Layout View (Recommended for maps with less than 50 symbols)
Topology	grid,star,ring,flow
CurrentTopology	grid
Criteria Properties	
name	172.16.33.1

Alarm Summary

Alarm Count					Category
0	0	0	1	3	Topology
0	0	0	3	0	Discovery

FIGURE 33-2 Creating a Map under Physical Networks



33_1_only - Smart View

✓ Map properties updated successfully

FIGURE 33-3 Map Created Successfully

- Configure Map - This allows the user to change the attributes of the create Map
- Delete Map - This deletes the Map the user is currently displaying

Note: *Do not delete a Map that is included by default, since the default Maps have information that is usually important to assess the network.*

- Add Symbol - Allows the user to add a symbol (image) to the map. This symbol can then be given attributes so that network changes can be highlighted using the image. NEED INFO - can give fault attributes to symbol?

33.2.4 Performance Monitoring

In previous releases, there was a separate tab for a Performance Monitoring frame. This has changed; the properties of a node in the Network Inventory view now include the appropriate graphs of statistics, and this is explained in the Network Inventory section, Network Inventory.

33.3 Network Maps

The Network Maps Tree has the following default nodes:

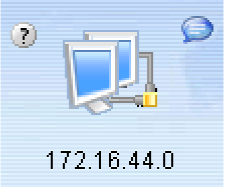
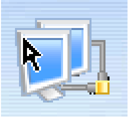
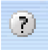
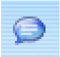
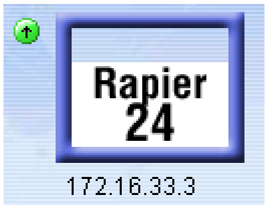
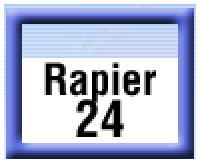
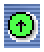
- Physical Network
- Routers
- Failed Nodes
- IP Network (usually highlighted when accessing the html interface for the first time)
- VLAN Network

The main map tasks are as follows, and explained in the next subsections:

- Drilling down the networks - The method to reach the exact, desired map element. This makes the monitoring easier.
- Managed properties - The method to get the details of a particular map symbol. It shows the editable properties and provides information on the allowable values for the properties.
- Query and Control the Device - From the map symbol the user can manage/unmanage the node and view events and alarms (which changes the function tab view). This is explained in detail below.

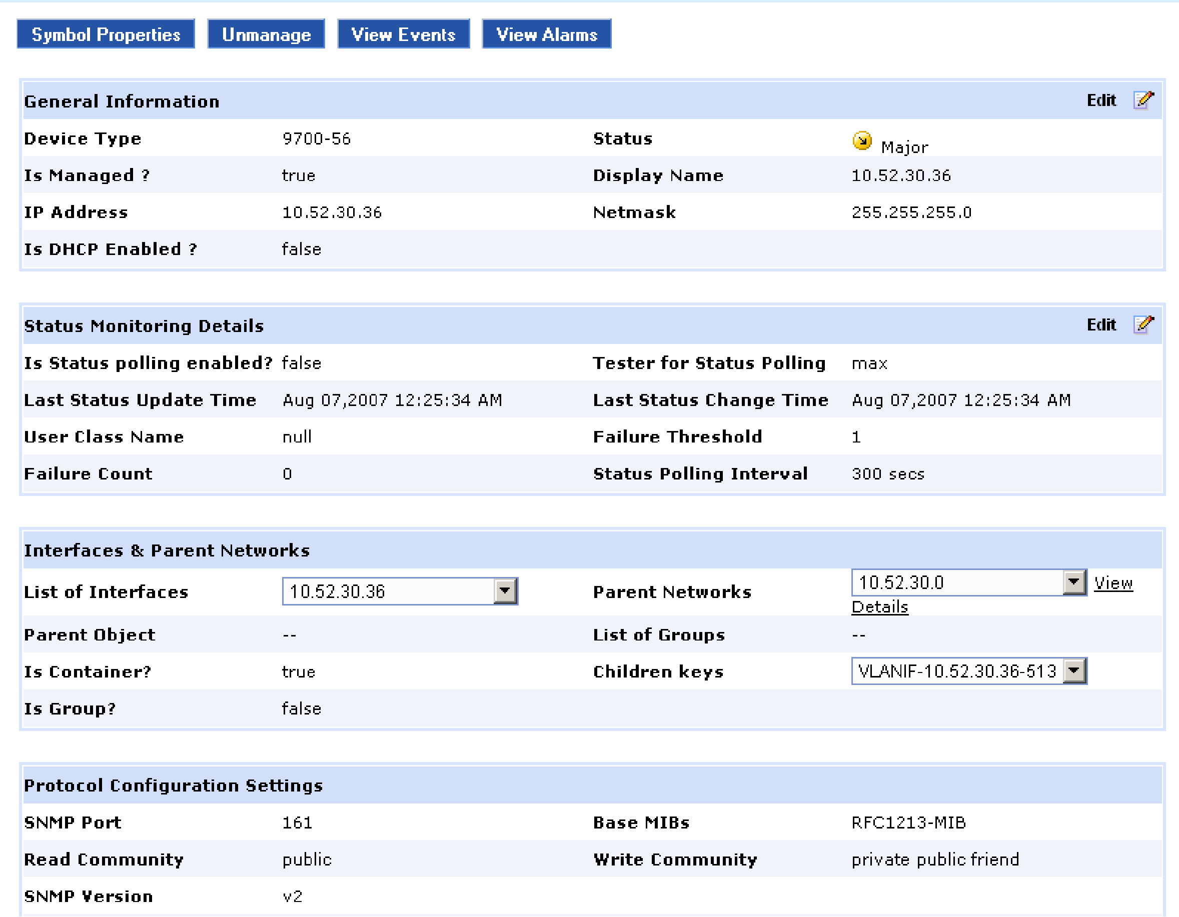
All icons accessed from the Network Maps tree have three buttons to perform these tasks. The following table explains these buttons.

TABLE 33-2 Actions available from Network Map and Device Icons

Icon	Icon Buttons	Action
		Clicking on this brings up the managed objects form, explained in Managed Properties Form.
		A state button, brings up the Fault Management View
		Brings up a smart (custom) view if one has been created.
		Clicking on this brings up the managed objects form, explained in Managed Properties Form.
		A state button, brings up the Fault Management View

33.3.1 Managed Properties Form

The necessary details of map symbols are available in a form called the Properties form. Refer to the following figure.



General Information

Device Type	9700-56	Status	Major
Is Managed ?	true	Display Name	10.52.30.36
IP Address	10.52.30.36	Netmask	255.255.255.0
Is DHCP Enabled ?	false		

Status Monitoring Details

Is Status polling enabled?	false	Tester for Status Polling	max
Last Status Update Time	Aug 07,2007 12:25:34 AM	Last Status Change Time	Aug 07,2007 12:25:34 AM
User Class Name	null	Failure Threshold	1
Failure Count	0	Status Polling Interval	300 secs

Interfaces & Parent Networks

List of Interfaces	10.52.30.36	Parent Networks	10.52.30.0 View Details
Parent Object	--	List of Groups	--
Is Container?	true	Children keys	VLANIF-10.52.30.36-513
Is Group?	false		

Protocol Configuration Settings

SNMP Port	161	Base MIBs	RFC1213-MIB
Read Community	public	Write Community	private public friend
SNMP Version	v2		

FIGURE 33-4 Map Properties Form (Network)

The properties are grouped as follows:

TABLE 33-3 Properties Form for Network Map Objects (Editable fields are in bold)

Type	Area	Detail
General	General Information	Device Type Status **Is Managed -** the result of Manage / Unmanage **Display Name -** what appears for the object
	Identification Details	IP Address Netmask Is DHCP Enabled?

TABLE 33-3 Properties Form for Network Map Objects (Editable fields are in bold)

Type	Area	Detail
Monitoring	Status Monitoring Details	**Is Status Polling Enabled** - whether the object status polling has been enabled for the object **Tester for Status Polling -** how the device is polled Last Status Update Time Last Status Change Time User Class Name **Failure Threshold -** number of failed polls before alert created Failure Count - how many times polling has failed **Status Polling Interval -**
Discovery	Discovery Setting	Discovery Status **Start / Resume Discovery**
Details	Nodes & Interface Details	List of Nodes List of Interfaces Sub Networks Sub Netmasks Parent Netmask Parent Network
Utilization	Currently Unused	CPU Memory Disk
Alarms		Status Failure Object Alarm Details Date / Time
Tabs	Symbol Properties Manage/Unmanage View Events View Alarms	

Some of the above properties are kept editable so that you can make changes as per your requirements. For example, the icon displayed for the map symbol can be changed to any other image by changing the icon name under General Properties.

33.3.2 Physical Network

The physical network lists all the device icons as described in Table 33-2, and is shown in the following figure.

Note: *As with the non-html interface, the RGs are not included in the Physical Network view; these are shown when the user chooses the relevant IP network.*

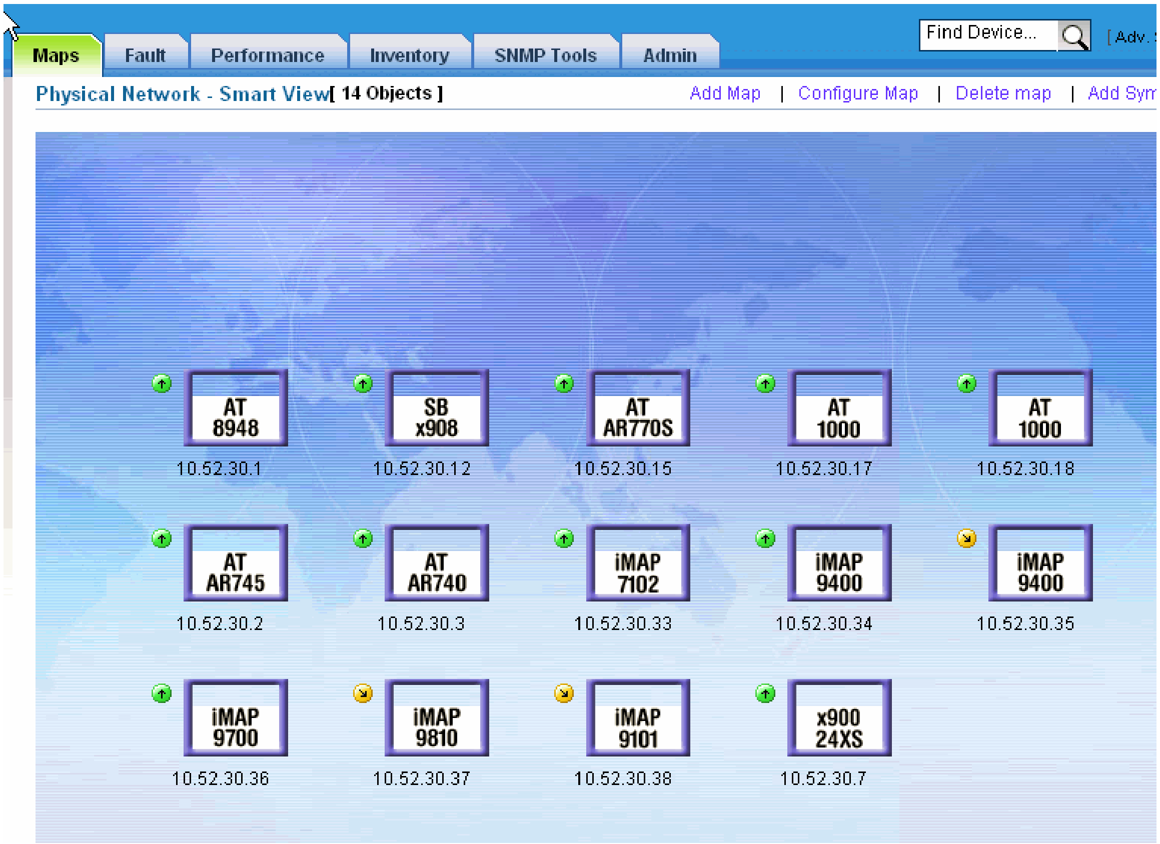
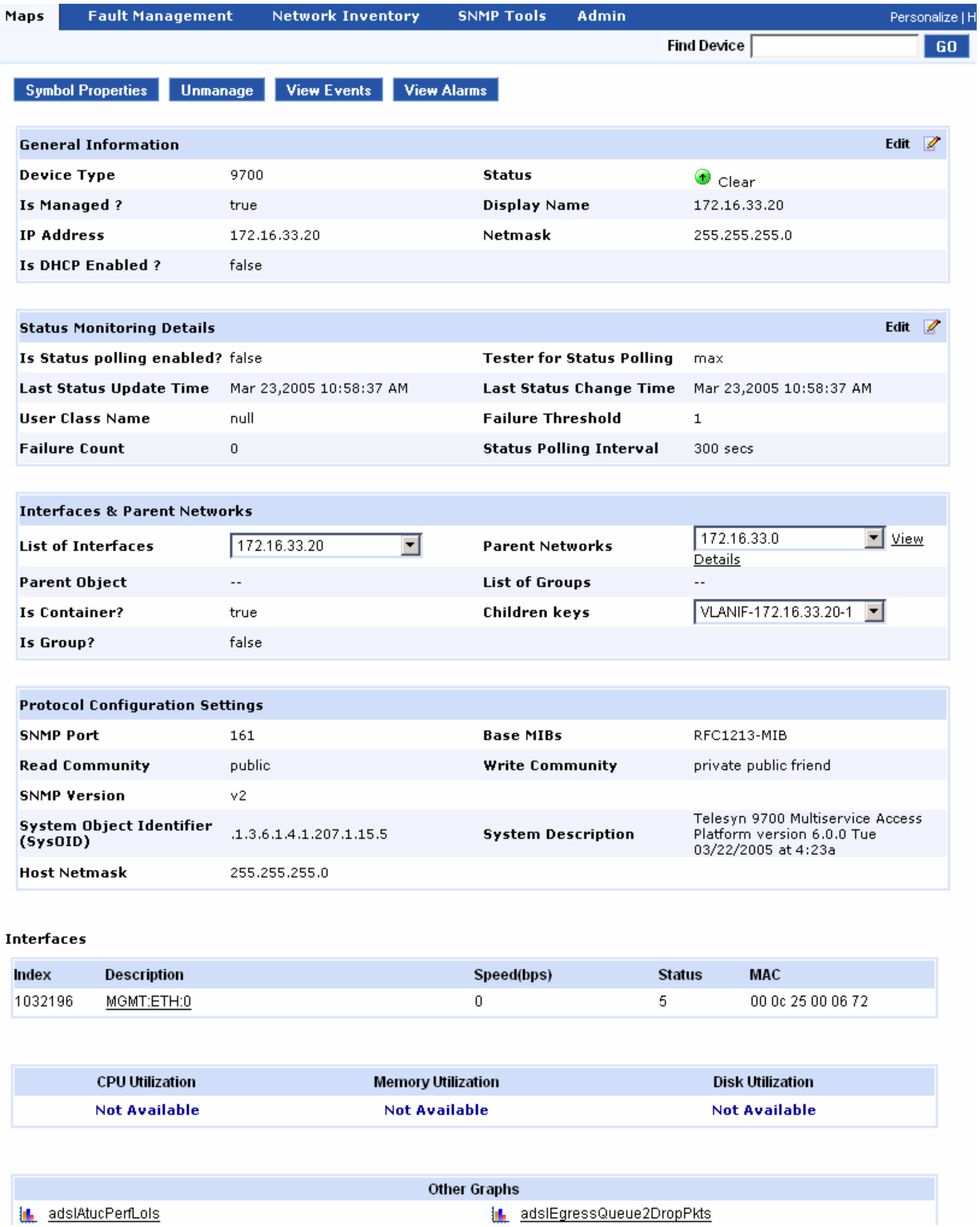


FIGURE 33-5 Physical Network - All Devices (Except iMG/RGs)

Clicking on the icon will bring up the Managed Object Properties Form, as shown in the following figure and table.



General Information			
Device Type	9700	Status	Clear
Is Managed ?	true	Display Name	172.16.33.20
IP Address	172.16.33.20	Netmask	255.255.255.0
Is DHCP Enabled ?	false		

Status Monitoring Details			
Is Status polling enabled?	false	Tester for Status Polling	max
Last Status Update Time	Mar 23,2005 10:58:37 AM	Last Status Change Time	Mar 23,2005 10:58:37 AM
User Class Name	null	Failure Threshold	1
Failure Count	0	Status Polling Interval	300 secs

Interfaces & Parent Networks			
List of Interfaces	172.16.33.20	Parent Networks	172.16.33.0 View Details
Parent Object	--	List of Groups	--
Is Container?	true	Children keys	VLANIF-172.16.33.20-1
Is Group?	false		

Protocol Configuration Settings			
SNMP Port	161	Base MIBs	RFC1213-MIB
Read Community	public	Write Community	private public friend
SNMP Version	v2		
System Object Identifier (SysOID)	.1.3.6.1.4.1.207.1.15.5	System Description	Telesyn 9700 Multiservice Access Platform version 6.0.0 Tue 03/22/2005 at 4:23a
Host Netmask	255.255.255.0		

Interfaces

Index	Description	Speed(bps)	Status	MAC
1032196	MGMT:ETH:0	0	5	00 0c 25 00 06 72

CPU Utilization	Memory Utilization	Disk Utilization
Not Available	Not Available	Not Available

Other Graphs

adslAtucPerfLols adslEgressQueue2DropPkts

FIGURE 33-6 Managed Object Properties Form for a Device

TABLE 33-4 Properties Form for Device Map Objects (Editable fields are in bold)

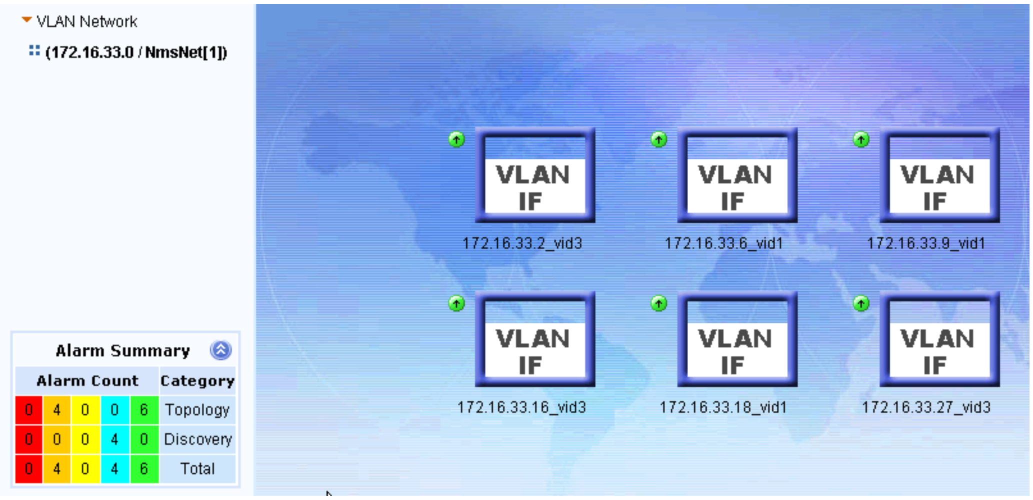
Type	Area	Detail
General	General Information	Device Type Status **Is Managed -** the result of Manage / Unmanage **Display Name -** what appears for the object
	Identification Details	IP Address Netmask Is DHCP Enabled?
Monitoring	Status Monitoring Details	**Is Status Polling Enabled** - whether the object status polling has been enabled for the object **Tester for Status Polling -** how the device is polled Last Status Update Time Last Status Change Time User Class Name **Failure Threshold -** number of failed polls before alert created Failure Count - how many times polling has failed **Status Polling Interval -**
Interfaces & Parent Networks		List of Interfaces Parent Network Parent Object List of Groups Is Container? Children Keys Is Group?
Protocol Configuration Settings		SNMP Port Base MIBs Read Community Write Community SNMP Version SysOID System Description Host Netmask
Interfaces		Index Description Speed Status MAC

TABLE 33-4 Properties Form for Device Map Objects (Editable fields are in bold)

Type	Area	Detail
Utilization		CPU Memory Disk
Other Graphs		Performance Monitoring

33.3.3 Other Network Maps

- Routers - These show only the devices configured as routers
- Failed Nodes - These show only those devices that have an Alarm with a severity
- VLAN Network - This shows the devices associated with each VLAN interface for the network chosen. Therefore, there will usually be a VLAN id repeated for the different devices it is configured on. Refer to the following figure.



Alarm Summary

Alarm Count					Category
0	4	0	0	6	Topology
0	0	0	4	0	Discovery
0	4	0	4	6	Total

FIGURE 33-7 VLAN Interfaces for the Selected Network

33.4 Fault Management (Events and Alarms)

33.4.1 Overview of Alarms

The devices connected with the NMS create various events. These events are converted (parsed) into alarms based on their significance. By default, the alarms are classified into five categories: Critical, Major, Minor, Warning, and Clear. This classification is based on the severity of the fault.

When you click the Alarms node in the Fault Management tree, the Alarms page is displayed, as shown in Figure 33-8. By default, it shows the following columns:

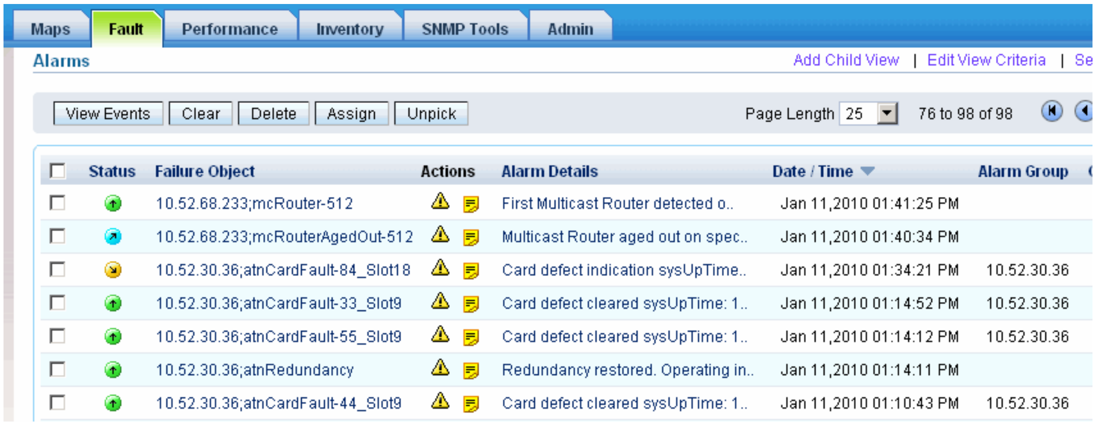
- Status - These are color-coded to indicate criticality in the same manner as events:
  - Red - Critical
  - Orange - Major
  - Yellow - Minor
  - Blue - Warning
  - Green - Clear
- Failure Object - Clicking on the link brings up the Alarm Details form.

- Actions - Using the icons, the user can acknowledge the alarm and annotate the alarm for future reference.
- Alarm Details - The text for the alarm.
- Date/Time - The date and time the alarm occurred.
- Alarm Group - ALarms can be assigned to a group when a parser is created. Groups are not used in the base NMS and are not shown in the HTML interface.
- Owner - The name of the login filled in the Alarm Details form.
- System Location - This is the value that was filled in the Managed Object Properties form.

The alarms are grouped by default for sets of 25 alarms in a page. This can be changed using the pull-down.

By clicking on a column header name, you can sort the list by the selected column information. When you click the name, an arrow shows the direction of the sort (up descending, down ascending). Each time you click the name, the sort direction toggles.

The following figure shows the alarm view.



☐	Status	Failure Object	Actions	Alarm Details	Date / Time ▼	Alarm Group
☐	●	10.52.68.233;mcRouter-512	⚠	First Multicast Router detected o..	Jan 11,2010 01:41:25 PM	
☐	●	10.52.68.233;mcRouterAgedOut-512	⚠	Multicast Router aged out on spec..	Jan 11,2010 01:40:34 PM	
☐	●	10.52.30.36;atnCardFault-84_Slot18	⚠	Card defect indication sysUpTime..	Jan 11,2010 01:34:21 PM	10.52.30.36
☐	●	10.52.30.36;atnCardFault-33_Slot9	⚠	Card defect cleared sysUpTime: 1..	Jan 11,2010 01:14:52 PM	10.52.30.36
☐	●	10.52.30.36;atnCardFault-55_Slot9	⚠	Card defect cleared sysUpTime: 1..	Jan 11,2010 01:14:12 PM	10.52.30.36
☐	●	10.52.30.36;atnRedundancy	⚠	Redundancy restored. Operating in..	Jan 11,2010 01:14:11 PM	
☐	●	10.52.30.36;atnCardFault-44_Slot9	⚠	Card defect cleared sysUpTime: 1..	Jan 11,2010 01:10:43 PM	10.52.30.36

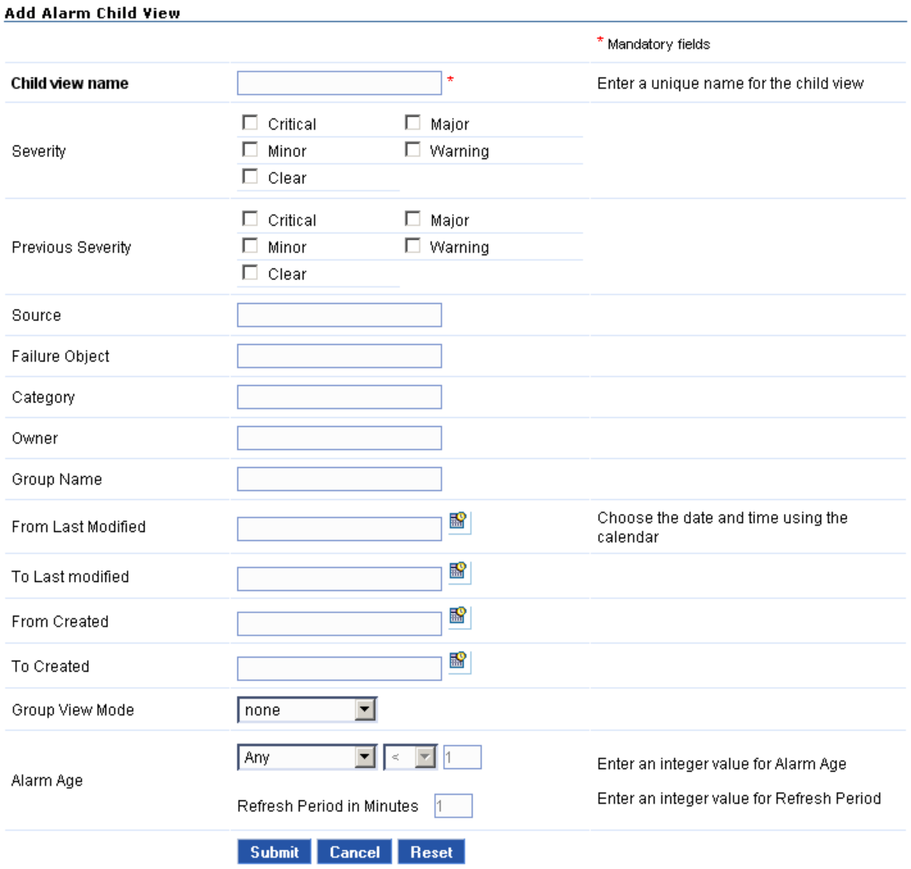
FIGURE 33-8 Alarm View for HTML Interface

33.4.2 Alarm View Options

The following options are available from the Alarm View. (These options are also used in the Events and System Logs Events view.)

33.4.2.1 Add Alarm Child View

This options allows the creation of a filtered view so that only certain alarms are shown. The following figure shows the Custom View Form.



Add Alarm Child View

* Mandatory fields

Child view name	____ *	Enter a unique name for the child view
Severity	□ Critical □ Major □ Minor □ Warning □ Clear	
Previous Severity	□ Critical □ Major □ Minor □ Warning □ Clear	
Source	____	
Failure Object	____	
Category	____	
Owner	____	
Group Name	____	
From Last Modified	____	Choose the date and time using the calendar
To Last modified	____	
From Created	____	
To Created	____	
Group View Mode	none	
Alarm Age	Any < 1 Refresh Period in Minutes 1	Enter an integer value for Alarm Age Enter an integer value for Refresh Period

Submit Cancel Reset

FIGURE 33-9 Creating an Alarm Child View

The name (Child view name) must be unique. For the criteria, refer to Alarms.

When the child view is created, it appears as a subnode to the Alarms node (where it appears cannot be changed).

The following table lists the properties.

TABLE 33-5 Alarm Custom View Properties

Property	Description
Custom View Name	The name of the custom view. This is a mandatory parameter. If you try to submit the form without mentioning the name, the message “No Custom View is mentioned” is displayed.
Severity	The severity of the event object, which indicates the criticality of the event. You can choose one of the severity (All, Major, Minor, Warning, Clear, Info, or Unknown) from the list box.
Previous Severity	The matching criteria based on the previous severity of the alarm.
Owner	The name of the owner with whom the alarm is associated.
Group	A group value based on which alarms are grouped in the client.
Message	An Alarm message for the particular custom view.
Category	The name of the category to which the alarm belongs. This could be used for better organization of alarms.

TABLE 33-5 Alarm Custom View Properties

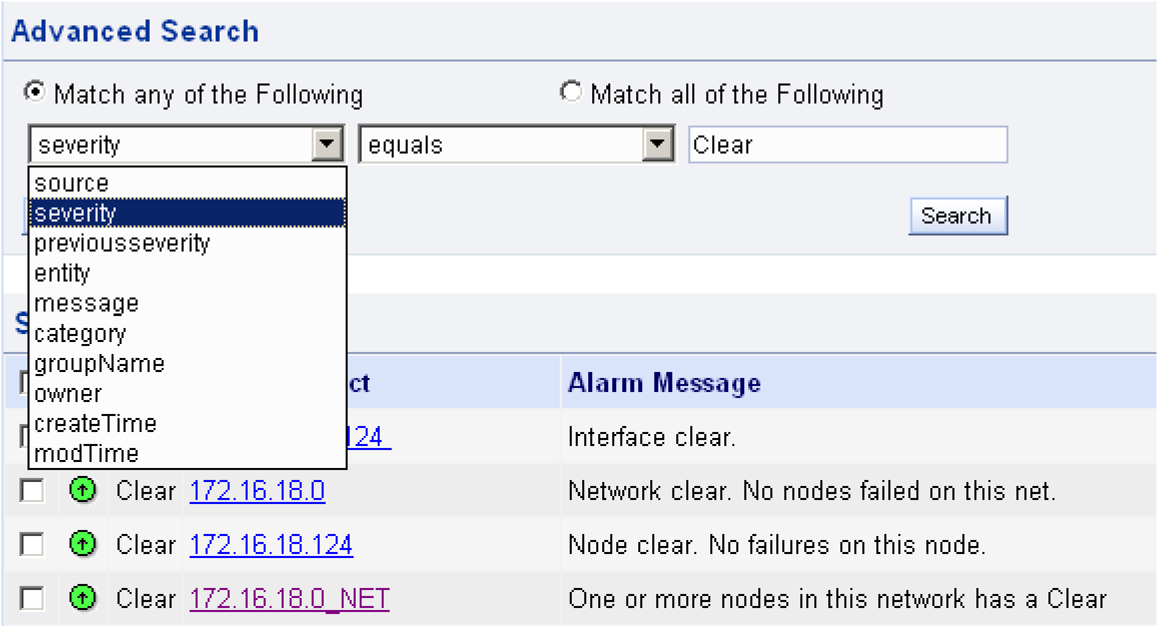
Property	Description
Failure Object	Information about the specific entity within the source of the event, which is primarily responsible for the occurrence of this event. The name of the failure object which caused the event to occur can be given in this field.
Source	Information about the source of the alarm. Alarms matching a particular source can be filtered out using this criterion.
From Date/ Time (Modified Time)	A from date and time for filtering out alarms modified from a particular date/time onward.
To Date/ Time (Modified Time)	A to date and time for filtering out alarms modified before a particular date/time.
From Date/ Time (Create Time)	A from date and time for filtering out alarms generated from a particular date/time onward.
To Date/ Time (Create Time)	A to date and time for filtering out alarms generated before a particular date/time.
GroupViewMode	The mode of grouping. It could be max, latest, or none. If max is selected, then alarms are grouped with the alarms of maximum criticality being shown at the top of the group. If latest is selected, then alarms are grouped with the latest alarm in a group shown at the top of the group. If GroupViewMode selected is none, then the alarms are not grouped.
Alarm Age	An age for filtering alarms based on the age of alarms. Age of an alarm denotes the time lapsed since the occurrence of the alarm in the NMS system.
Refresh Period (in Min.)	The frequency at which the latest alarms should be updated in the alarm browser from the database.

33.4.2.2 Edit View Criteria

This option allows the user to modify the criteria for the selected view. The criteria is the same as when creating a custom view.

33.4.2.3 Search

The search option allows the user to further refine a view by listing columns and the criteria the column must match. The More button allows more that one column to be used, and the Match radio buttons allow an OR (any) or AND (all) criteria to be set. Refer to the following figure, which shows a search based on the severity of Clear.



Advanced Search

● Match any of the Following ○ Match all of the Following

severity ▼ equals ▼ Clear

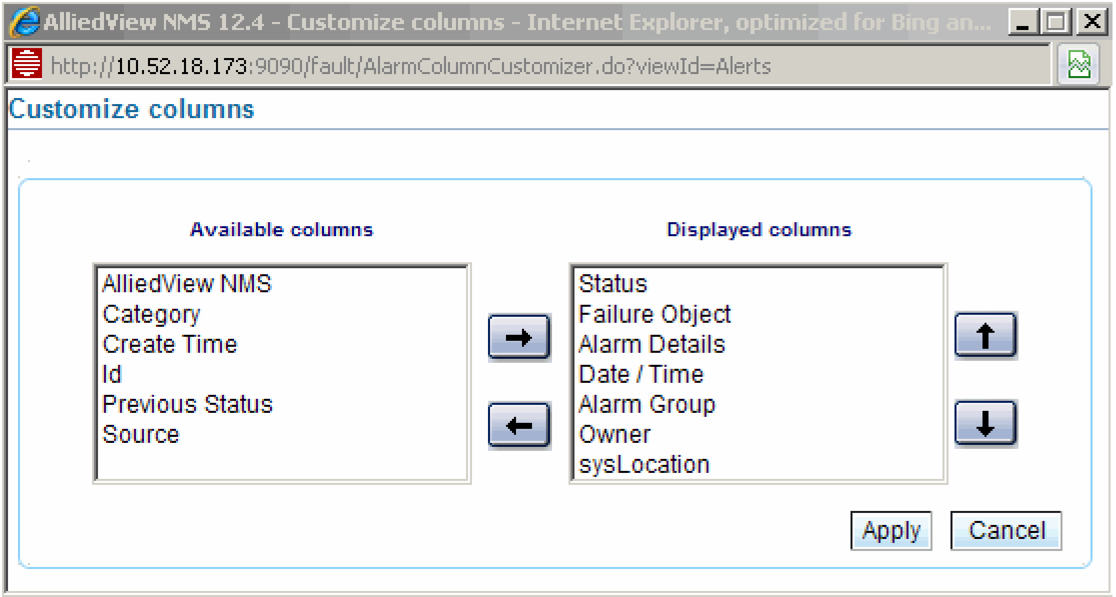
			ct	Alarm Message
□			124	Interface clear.
□	●	Clear	172.16.18.0	Network clear. No nodes failed on this net.
□	●	Clear	172.16.18.124	Node clear. No failures on this node.
□	●	Clear	172.16.18.0_NET	One or more nodes in this network has a Clear

FIGURE 33-10 Advanced Search for a View

For the text values for criteria, refer to Matching Criteria.

33.4.2.4 Customize Columns

This options allows the user to control which columns are displayed in a view. The user moves (using the right and left arrows) the columns to be displayed. To control the order, select one of the Displayed columns and use the up and down arrows to control where it is placed. Refer to the following figure.



AlliedView NMS 12.4 - Customize columns - Internet Explorer, optimized for Bing an...

http://10.52.18.173:9090/fault/AlarmColumnCustomizer.do?viewId=Alerts

Customize columns

Available columns	Displayed columns
AlliedView NMS	Status
Category	Failure Object
Create Time	Alarm Details
Id	Date / Time
Previous Status	Alarm Group
Source	Owner
	sysLocation

33.4.2.5 Operations

After checking the tic box for one or more alarms the user can choose one of the following actions:

- **View Events** - displays the list of events for the object that had created the alarm.

- Clear - This will set the status to Clear and show what the previous status was.
- Delete - Deletes the alarm (after a confirmation window).
- Pickup - Allows a user to be associated with an alarm.
- Unpick - Disassociates a user with an alarm.

Note: If any of the parameter fields (except Custom View Name) is left blank, the default value all is assigned.

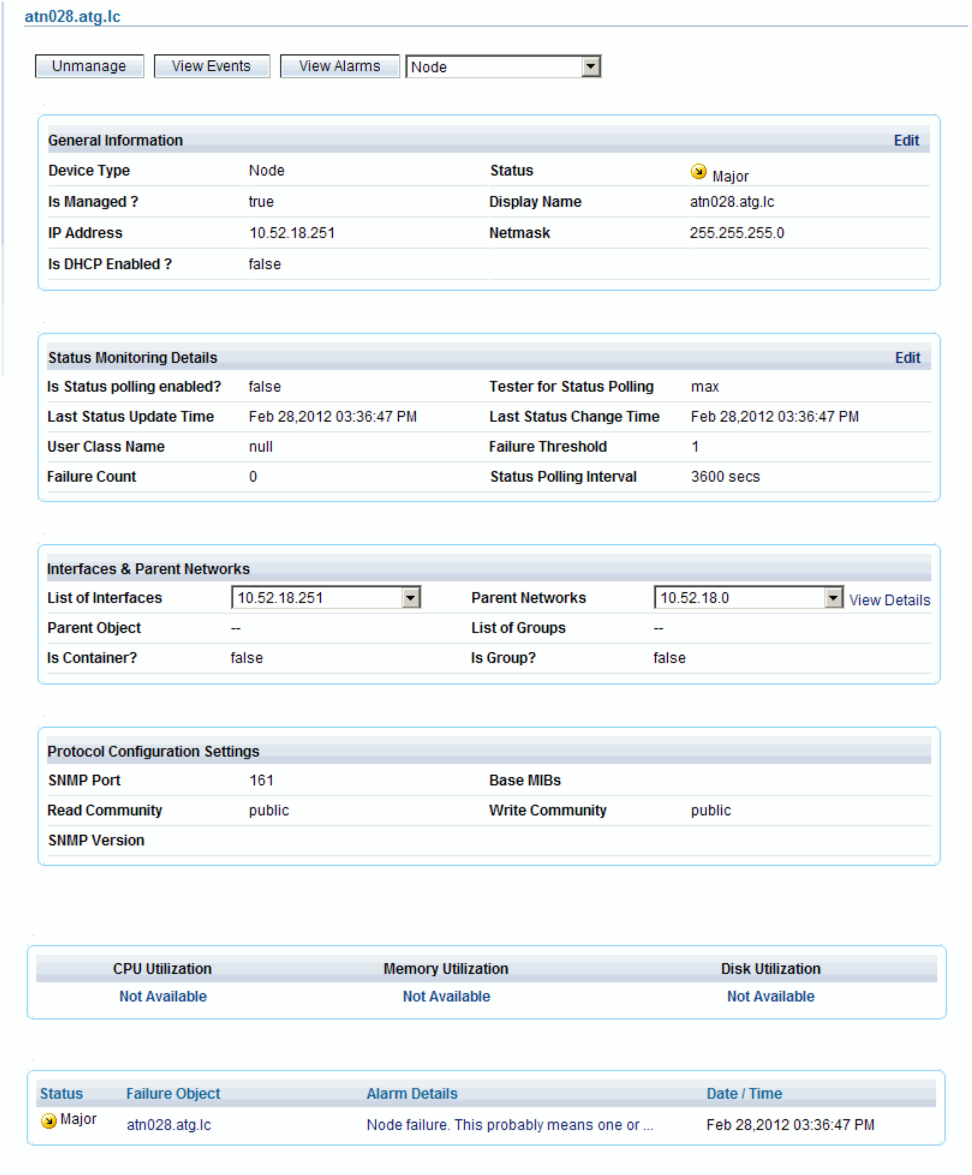
33.4.3 Alarm Properties (Details)

After clicking on the link for the Failure Object, the user will see the Network Inventory Window with the MO Objects properties form. The properties of this form are explained in

The user has the following options:

- Unmanage
- View Events
- View Alarms

If the object is a Network, a list of alarms is listed at the bottom of the window, and the user can query the individual failure object. For details on the Network Inventory frame, refer to Network Inventory.



General Information Edit

Device Type	Node	Status	● Major
Is Managed ?	true	Display Name	atn028.atg.lc
IP Address	10.52.18.251	Netmask	255.255.255.0
Is DHCP Enabled ?	false		

Status Monitoring Details Edit

Is Status polling enabled?	false	Tester for Status Polling	max
Last Status Update Time	Feb 28,2012 03:36:47 PM	Last Status Change Time	Feb 28,2012 03:36:47 PM
User Class Name	null	Failure Threshold	1
Failure Count	0	Status Polling Interval	3600 secs

Interfaces & Parent Networks

List of Interfaces	10.52.18.251	Parent Networks	10.52.18.0 View Details
Parent Object	--	List of Groups	--
Is Container?	false	Is Group?	false

Protocol Configuration Settings

SNMP Port	161	Base MIBs	
Read Community	public	Write Community	public
SNMP Version			

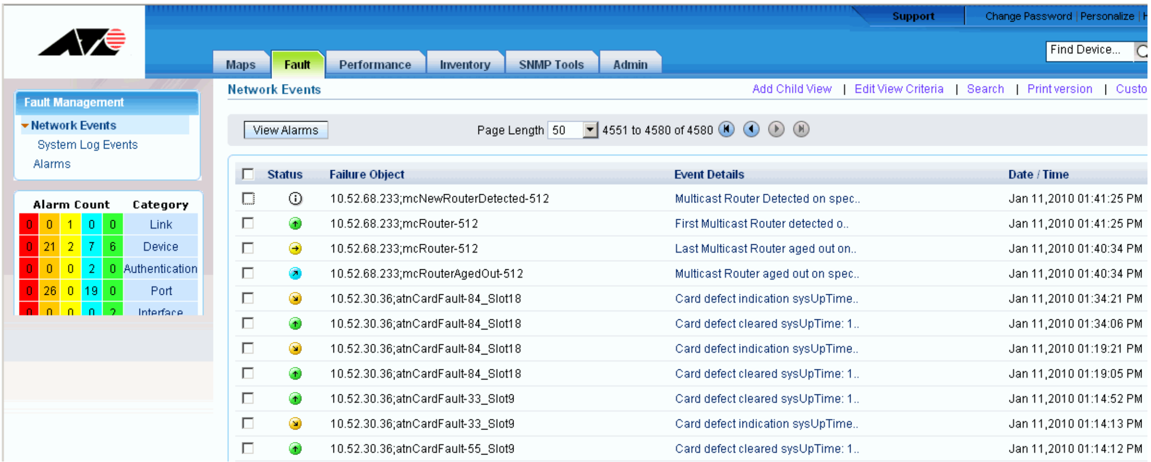
CPU Utilization	Memory Utilization	Disk Utilization
Not Available	Not Available	Not Available

Status	Failure Object	Alarm Details	Date / Time
● Major	atn028.atg.lc	Node failure. This probably means one or ...	Feb 28,2012 03:36:47 PM

FIGURE 33-11 Alarm Details Form

33.4.4 Overview of Network Events

Events are simply the complete sets of notifications from the network. They are basically of two types: External and Internal events. External events are actions or notifications that are external to the NMS (for example, Traps, which are basic notifications from the SNMP agents or management applications). Internal events are notifications that are generated by the NMS during data polling and status polling (for example, threshold events and status events). The following figure shows the default Event view.



Alarm Count					Category
0	0	1	0	0	Link
0	21	2	7	6	Device
0	0	0	2	0	Authentication
0	26	0	19	0	Port
0	0	0	0	2	Interface

□	Status	Failure Object	Event Details	Date / Time
□	ⓘ	10.52.68.233;mcNewRouterDetected-512	Multicast Router Detected on spec..	Jan 11,2010 01:41:25 PM
□	↑	10.52.68.233;mcRouter-512	First Multicast Router detected o..	Jan 11,2010 01:41:25 PM
□	→	10.52.68.233;mcRouter-512	Last Multicast Router aged out on..	Jan 11,2010 01:40:34 PM
□	↗	10.52.68.233;mcRouterAgedOut-512	Multicast Router aged out on spec..	Jan 11,2010 01:40:34 PM
□	↘	10.52.30.36;atnCardFault-84_Slot18	Card defect indication sysUpTime..	Jan 11,2010 01:34:21 PM
□	↑	10.52.30.36;atnCardFault-84_Slot18	Card defect cleared sysUpTime: 1..	Jan 11,2010 01:34:06 PM
□	↘	10.52.30.36;atnCardFault-84_Slot18	Card defect indication sysUpTime..	Jan 11,2010 01:19:21 PM
□	↑	10.52.30.36;atnCardFault-84_Slot18	Card defect cleared sysUpTime: 1..	Jan 11,2010 01:19:05 PM
□	↑	10.52.30.36;atnCardFault-33_Slot9	Card defect cleared sysUpTime: 1..	Jan 11,2010 01:14:52 PM
□	↘	10.52.30.36;atnCardFault-33_Slot9	Card defect indication sysUpTime..	Jan 11,2010 01:14:13 PM
□	↑	10.52.30.36;atnCardFault-55_Slot9	Card defect cleared sysUpTime: 1..	Jan 11,2010 01:14:12 PM

FIGURE 33-12 Network Events View for html Interface

33.4.5 Event View Options

The options for the event view are the same as the alarm view, explained in Alarm View Options.

33.4.6 Viewing Event Details

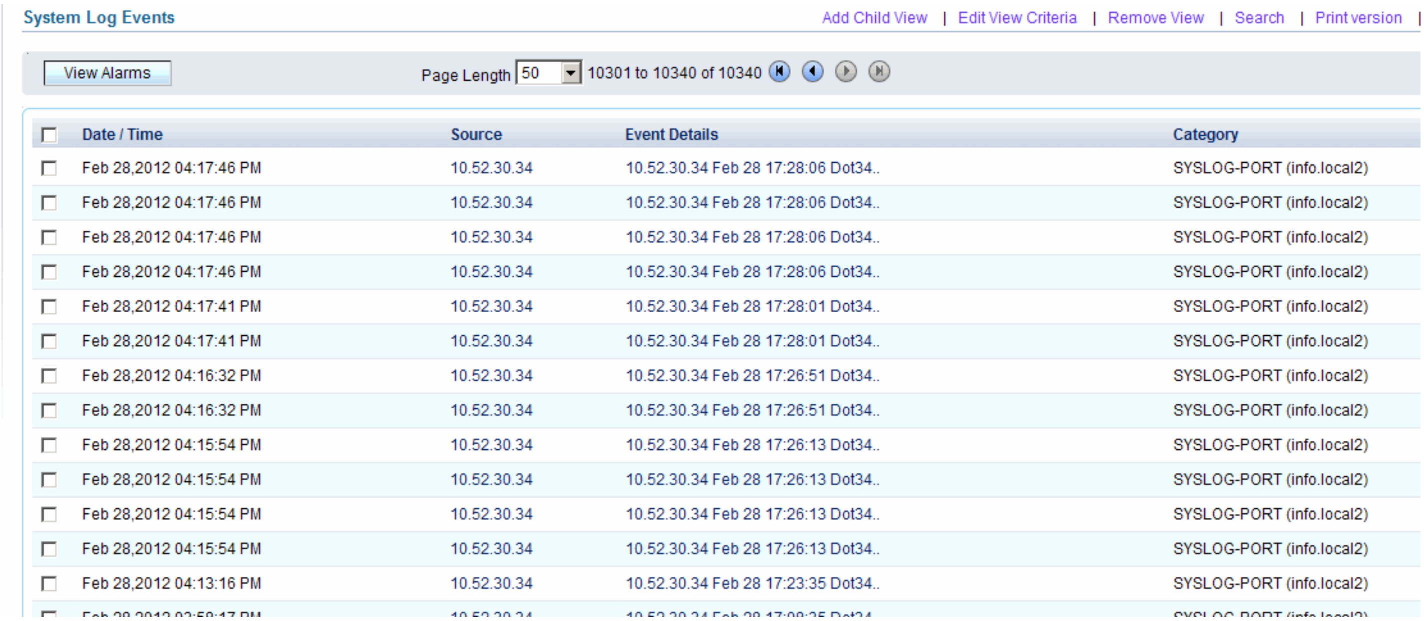
The Event Details page is accessed by choosing the Source field, and has the same fields as the Alarm view, explained in Alarm Properties (Details).

33.4.7 System Log Events View

The relationship between the components that provide system logs is as follows:

- The filtering of logs produced by the device that are sent to the NMS is controlled by applying log filters.
- The logs that are displayed in the **System Log Events** tree node (Under **Network Events**) are controlled through configuring the system log server.

At the html GUI, the initial System Log Events view lists the logs that the NMS has been set up to filter and display. Refer to the following figure.



System Log Events

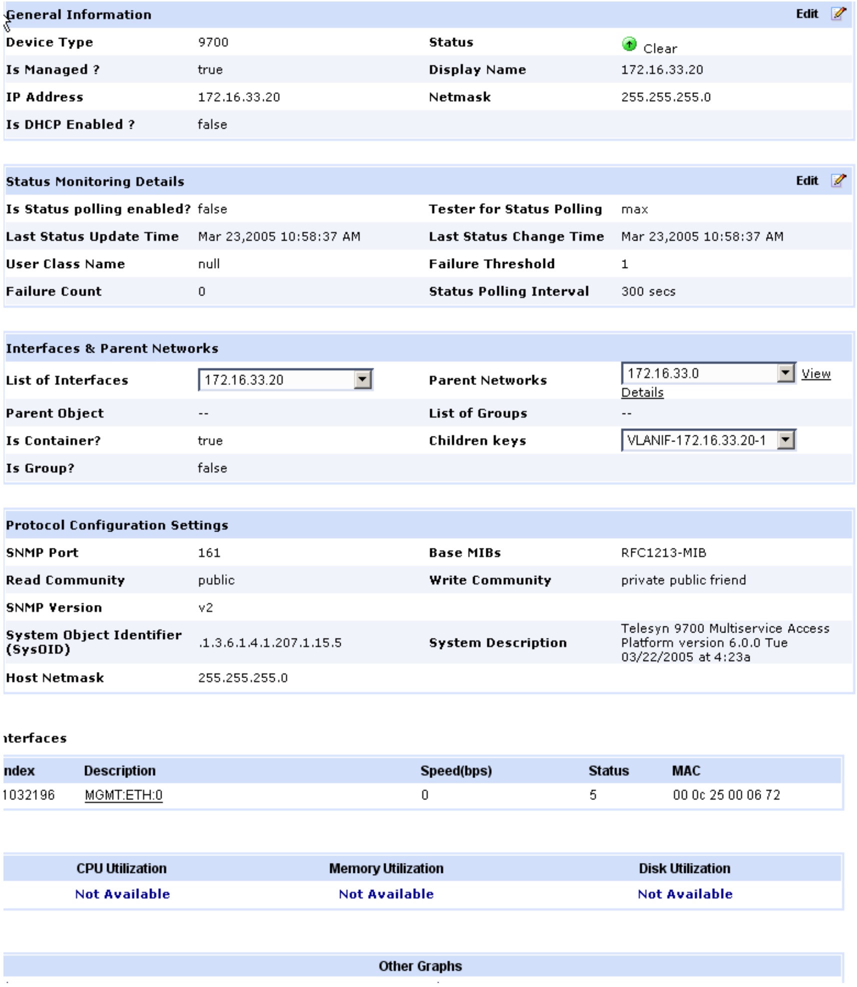
Add Child View | Edit View Criteria | Remove View | Search | Print version |
View Alarms
Page Length 50
10301 to 10340 of 10340

□	Date / Time	Source	Event Details	Category
□	Feb 28,2012 04:17:46 PM	10.52.30.34	10.52.30.34 Feb 28 17:28:06 Dot34..	SYSLOG-PORT (info.local2)
□	Feb 28,2012 04:17:46 PM	10.52.30.34	10.52.30.34 Feb 28 17:28:06 Dot34..	SYSLOG-PORT (info.local2)
□	Feb 28,2012 04:17:46 PM	10.52.30.34	10.52.30.34 Feb 28 17:28:06 Dot34..	SYSLOG-PORT (info.local2)
□	Feb 28,2012 04:17:46 PM	10.52.30.34	10.52.30.34 Feb 28 17:28:06 Dot34..	SYSLOG-PORT (info.local2)
□	Feb 28,2012 04:17:41 PM	10.52.30.34	10.52.30.34 Feb 28 17:28:01 Dot34..	SYSLOG-PORT (info.local2)
□	Feb 28,2012 04:17:41 PM	10.52.30.34	10.52.30.34 Feb 28 17:28:01 Dot34..	SYSLOG-PORT (info.local2)
□	Feb 28,2012 04:16:32 PM	10.52.30.34	10.52.30.34 Feb 28 17:26:51 Dot34..	SYSLOG-PORT (info.local2)
□	Feb 28,2012 04:16:32 PM	10.52.30.34	10.52.30.34 Feb 28 17:26:51 Dot34..	SYSLOG-PORT (info.local2)
□	Feb 28,2012 04:15:54 PM	10.52.30.34	10.52.30.34 Feb 28 17:26:13 Dot34..	SYSLOG-PORT (info.local2)
□	Feb 28,2012 04:15:54 PM	10.52.30.34	10.52.30.34 Feb 28 17:26:13 Dot34..	SYSLOG-PORT (info.local2)
□	Feb 28,2012 04:15:54 PM	10.52.30.34	10.52.30.34 Feb 28 17:26:13 Dot34..	SYSLOG-PORT (info.local2)
□	Feb 28,2012 04:15:54 PM	10.52.30.34	10.52.30.34 Feb 28 17:26:13 Dot34..	SYSLOG-PORT (info.local2)
□	Feb 28,2012 04:13:16 PM	10.52.30.34	10.52.30.34 Feb 28 17:23:35 Dot34..	SYSLOG-PORT (info.local2)
□	Feb 28,2012 03:58:17 PM	10.52.30.34	10.52.30.34 Feb 28 17:09:25 Dot34..	SYSLOG-PORT (info.local2)

FIGURE 33-13 Initial System Log Events View

The properties of the System Log Events are shown by clicking on the **Source** field, and are almost the same as the Alarm properties as explained in Alarm Properties (Details).

Refer to the following figure.



General Information Edit

Device Type	9700	Status	Clear
Is Managed ?	true	Display Name	172.16.33.20
IP Address	172.16.33.20	Netmask	255.255.255.0
Is DHCP Enabled ?	false		

Status Monitoring Details Edit

Is Status polling enabled?	false	Tester for Status Polling	max
Last Status Update Time	Mar 23,2005 10:58:37 AM	Last Status Change Time	Mar 23,2005 10:58:37 AM
User Class Name	null	Failure Threshold	1
Failure Count	0	Status Polling Interval	300 secs

Interfaces & Parent Networks

List of Interfaces	172.16.33.20	Parent Networks	172.16.33.0 View Details
Parent Object	--	List of Groups	--
Is Container?	true	Children keys	VLANIF-172.16.33.20-1
Is Group?	false		

Protocol Configuration Settings

SNMP Port	161	Base MIBs	RFC1213-MIB
Read Community	public	Write Community	private public friend
SNMP Version	v2		
System Object Identifier (SysOID)	.1.3.6.1.4.1.207.1.15.5	System Description	Telesyn 9700 Multiservice Access Platform version 6.0.0 Tue 03/22/2005 at 4:23a
Host Netmask	255.255.255.0		

nterfaces

ndex	Description	Speed(bps)	Status	MAC
1032196	MGMT:ETH:0	0	5	00 0c 25 00 06 72

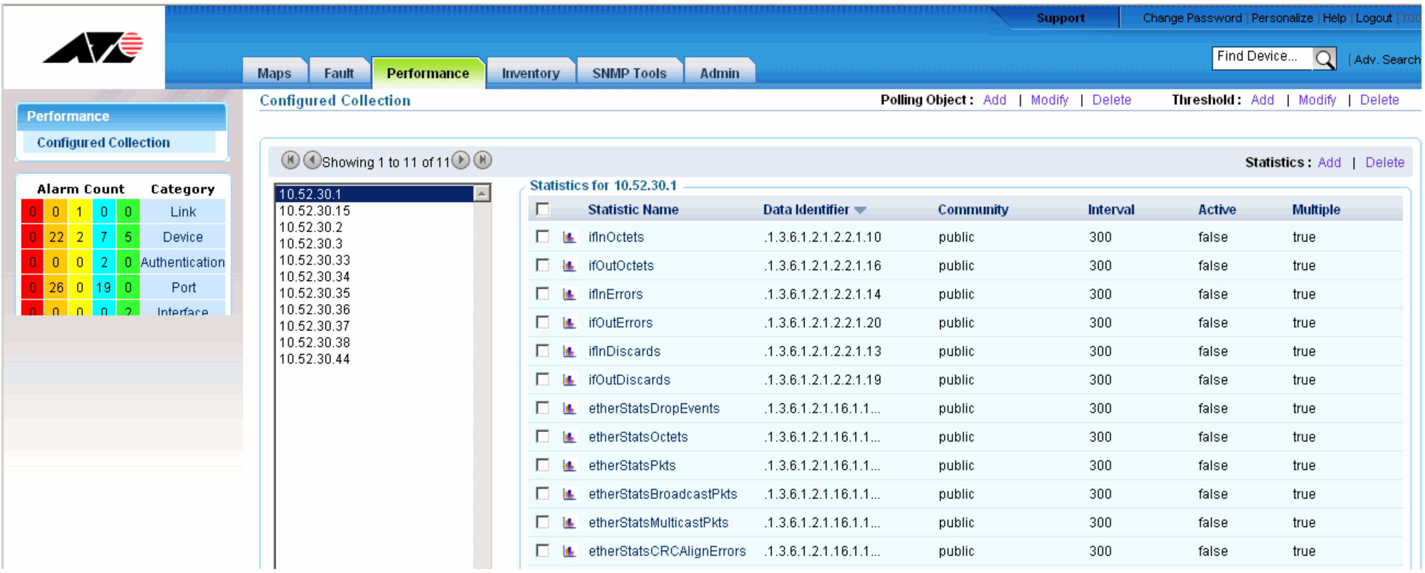
CPU Utilization	Memory Utilization	Disk Utilization
Not Available	Not Available	Not Available

Other Graphs

FIGURE 33-14 SYSLOG Event Properties

33.5 Performance

To control statistics that are collected and reported the user can select a host and then add, modify, or delete a statistic. Refer to the following figure.


Support
Change Password | Personalize | Help | Logout
Maps
Fault
Performance
Inventory
SNMP Tools
Admin
Find Device...
Adv. Search
Performance
Configured Collection
Polling Object : Add | Modify | Delete
Threshold : Add | Modify | Delete
Statistics : Add | Delete

Configured Collection

Alarm Count					Category
0	0	1	0	0	Link
0	22	2	7	5	Device
0	0	0	2	0	Authentication
0	26	0	19	0	Port
0	0	0	0	2	Interface

Showing 1 to 11 of 11

10.52.30.1
10.52.30.15
10.52.30.2
10.52.30.3
10.52.30.33
10.52.30.34
10.52.30.35
10.52.30.36
10.52.30.37
10.52.30.38
10.52.30.44

Statistics for 10.52.30.1

□	Statistic Name	Data Identifier	Community	Interval	Active	Multiple
□	ifInOctets	.1.3.6.1.2.1.2.2.1.10	public	300	false	true
□	ifOutOctets	.1.3.6.1.2.1.2.2.1.16	public	300	false	true
□	ifInErrors	.1.3.6.1.2.1.2.2.1.14	public	300	false	true
□	ifOutErrors	.1.3.6.1.2.1.2.2.1.20	public	300	false	true
□	ifInDiscards	.1.3.6.1.2.1.2.2.1.13	public	300	false	true
□	ifOutDiscards	.1.3.6.1.2.1.2.2.1.19	public	300	false	true
□	etherStatsDropEvents	.1.3.6.1.2.1.16.1.1...	public	300	false	true
□	etherStatsOctets	.1.3.6.1.2.1.16.1.1...	public	300	false	true
□	etherStatsPkts	.1.3.6.1.2.1.16.1.1...	public	300	false	true
□	etherStatsBroadcastPkts	.1.3.6.1.2.1.16.1.1...	public	300	false	true
□	etherStatsMulticastPkts	.1.3.6.1.2.1.16.1.1...	public	300	false	true
□	etherStatsCRCAlignErrors	.1.3.6.1.2.1.16.1.1...	public	300	false	true

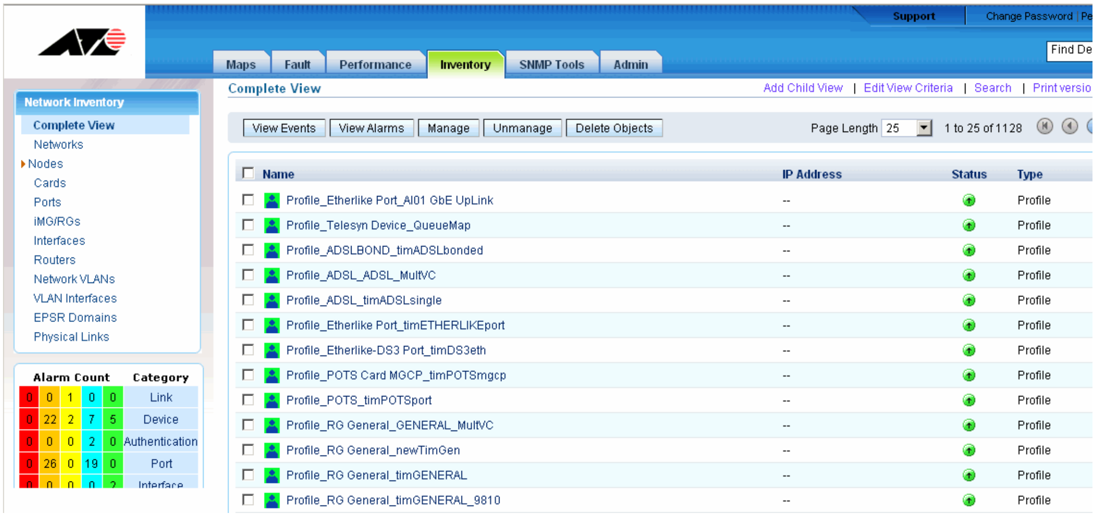
FIGURE 33-15 Controlling Performance Data

33.6 Network Inventory

The Network Inventory, sometimes referred to as the topology database, is the repository of all of the data for all of the objects managed by the AlliedView NMS. A network, therefore, is an object that contains one or more nodes, each of which in turn contains one or more interfaces. The properties of all these objects are maintained in the Network Inventory. These are shown under the Network Inventory node in the tree.

The inventory views for all of these objects are based on a table view, where each row pertains to a managed object. Clicking on the column name sorts the table data according to the information in the selected (clicked) column.

The following figures and tables show each object view, the icons that are used, and descriptions of the table columns.



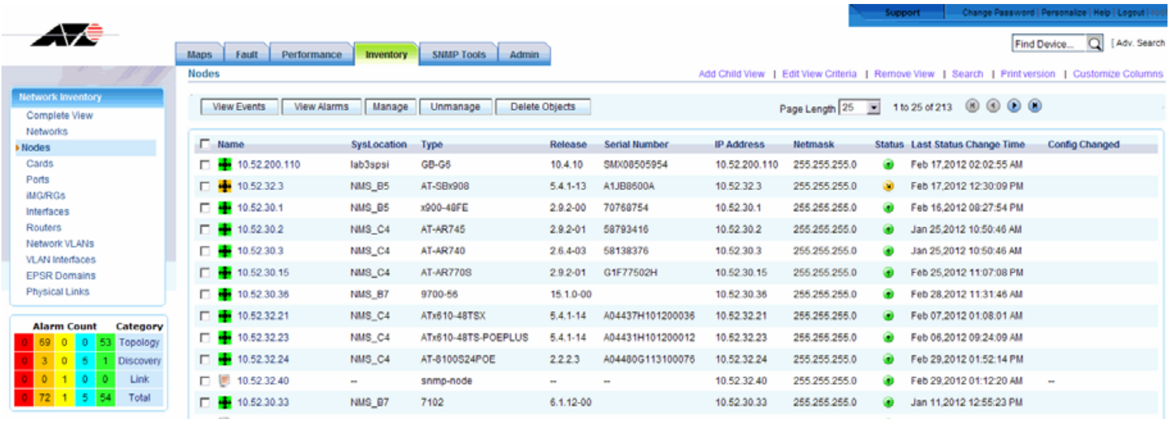
Alarm Count					Category
0	0	1	0	0	Link
0	22	2	7	5	Device
0	0	0	2	0	Authentication
0	26	0	19	0	Port
0	0	0	0	2	Interface

□	Name	IP Address	Status	Type
□	Profile_Etherlike Port_AI01 GbE UpLink	--	●	Profile
□	Profile_Telesyn Device_QueueMap	--	●	Profile
□	Profile_ADSLBOND_timADSLbonded	--	●	Profile
□	Profile_ADSL_ADSL_MultVC	--	●	Profile
□	Profile_ADSL_timADSLsingle	--	●	Profile
□	Profile_Etherlike Port_timETHERLIKEport	--	●	Profile
□	Profile_Etherlike-DS3 Port_timDS3eth	--	●	Profile
□	Profile_POTS Card MGCP_timPOTSmgcp	--	●	Profile
□	Profile_POTS_timPOTSport	--	●	Profile
□	Profile_RG General_GENERAL_MultVC	--	●	Profile
□	Profile_RG General_newTimGen	--	●	Profile
□	Profile_RG General_timGENERAL	--	●	Profile
□	Profile_RG General_timGENERAL_9810	--	●	Profile

FIGURE 33-16 Network Inventory View (HTML)

TABLE 33-6 Network View Columns

Column	Meaning
Name	The object name. The icon to the left of the name ( ) is the icon for a network object, which is the object type, where the icon color depicts current criticality state of the object. Left-clicking the name brings up the Object Details form. The arrow to the right of the name (») brings up a menu of appropriate actions (Manage/ Unmanage). Left-clicking the arrow brings up the menu.
IPAddress	The object IP address. Every object has a unique IP address.
Status	The alert status.
Type	One of the types listed in the Network Inventory tree
NetMask	The object subnetwork or network category.



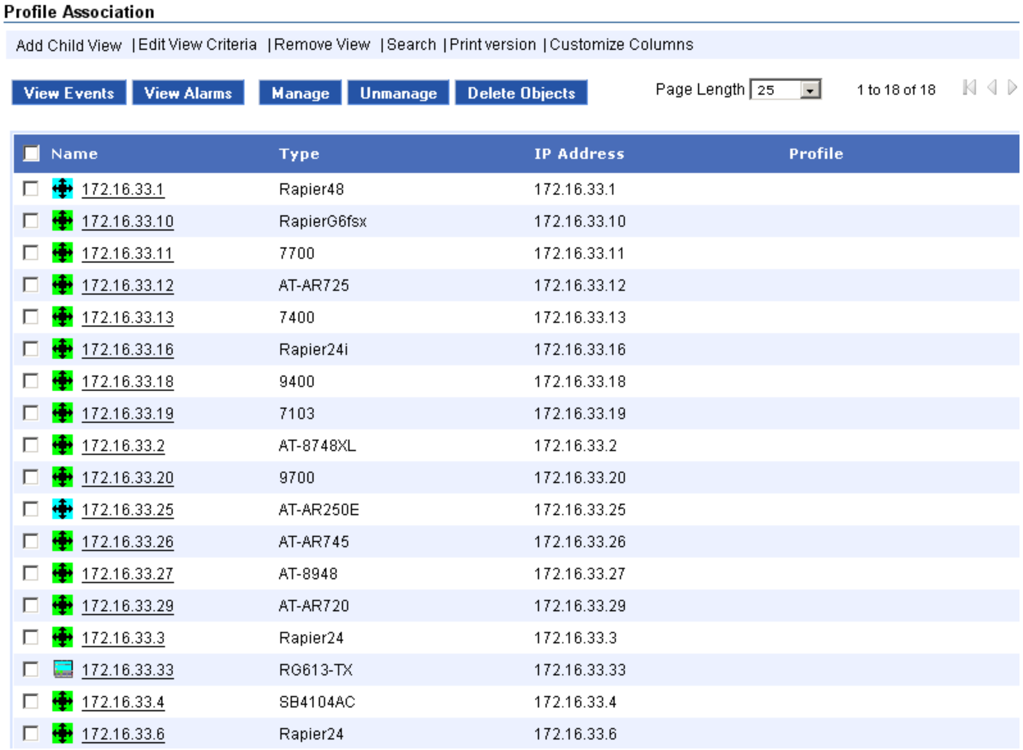
Alarm Count					Category
0	69	0	0	53	Topology
0	3	0	5	1	Discovery
0	0	1	0	0	Link
0	72	1	5	54	Total

□	Name	SysLocation	Type	Release	Serial Number	IP Address	Netmask	Status	Last Status Change Time	Config Changed
□	10.52.200.110	lab3spsi	GB-G6	10.4.10	SMX08505954	10.52.200.110	255.255.255.0	●	Feb 17,2012 02:02:55 AM	
□	10.52.32.3	NMS_B5	AT-SBx908	5.4.1-13	A1JB8600A	10.52.32.3	255.255.255.0	●	Feb 17,2012 12:30:09 PM	
□	10.52.30.1	NMS_B5	x900-48FE	2.9.2-00	70768754	10.52.30.1	255.255.255.0	●	Feb 16,2012 08:27:54 PM	
□	10.52.30.2	NMS_C4	AT-AR745	2.9.2-01	58793416	10.52.30.2	255.255.255.0	●	Jan 25,2012 10:50:46 AM	
□	10.52.30.3	NMS_C4	AT-AR740	2.6.4-03	58138376	10.52.30.3	255.255.255.0	●	Jan 25,2012 10:50:46 AM	
□	10.52.30.15	NMS_C4	AT-AR770S	2.9.2-01	G1F77502H	10.52.30.15	255.255.255.0	●	Feb 25,2012 11:07:08 PM	
□	10.52.30.36	NMS_B7	9700-56	15.1.0-00		10.52.30.36	255.255.255.0	●	Feb 28,2012 11:31:46 AM	
□	10.52.32.21	NMS_C4	ATx610-48TSX	5.4.1-14	A04437H101200036	10.52.32.21	255.255.255.0	●	Feb 07,2012 01:08:01 AM	
□	10.52.32.23	NMS_C4	ATx610-48TS-POEPLUS	5.4.1-14	A04431H101200012	10.52.32.23	255.255.255.0	●	Feb 06,2012 09:24:09 AM	
□	10.52.32.24	NMS_C4	AT-8100S24POE	2.2.2.3	A04480G113100076	10.52.32.24	255.255.255.0	●	Feb 29,2012 01:52:14 PM	
□	10.52.32.40	--	snmp-node	--	--	10.52.32.40	255.255.255.0	●	Feb 29,2012 01:12:20 AM	--
□	10.52.30.33	NMS_B7	7102	6.1.12-00		10.52.30.33	255.255.255.0	●	Jan 11,2012 12:55:23 PM	

FIGURE 33-17 Node View (HTML)

TABLE 33-7 Node View Columns

Column	Meaning
Name	The object name. The icon to the left of the name (✚) is the icon for a network node object, which is the object type, where the icon color depicts current criticality state of the object. Left-clicking the name brings up the Object Details form. The arrow to the right of the name (») brings up a menu of appropriate actions (Manage/ Unmanage). Left-clicking the arrow brings up the menu.
SysLocation	The MO property to identify a location
Type	The device type (the type of AT device).
Release	The software release the device is running.
Serial Number	The unique name given by AT to identify the device.
IPAddress	The object IP address.
NetMask	The object subnetwork or network category.
Status	The alert status.
Last Status Time Change	The date and time at which the object information was last updated.
Config Changed	The last time the device configuration was changed.



Profile Association

Add Child View | Edit View Criteria | Remove View | Search | Print version | Customize Columns

View Events | View Alarms | Manage | Unmanage | Delete Objects

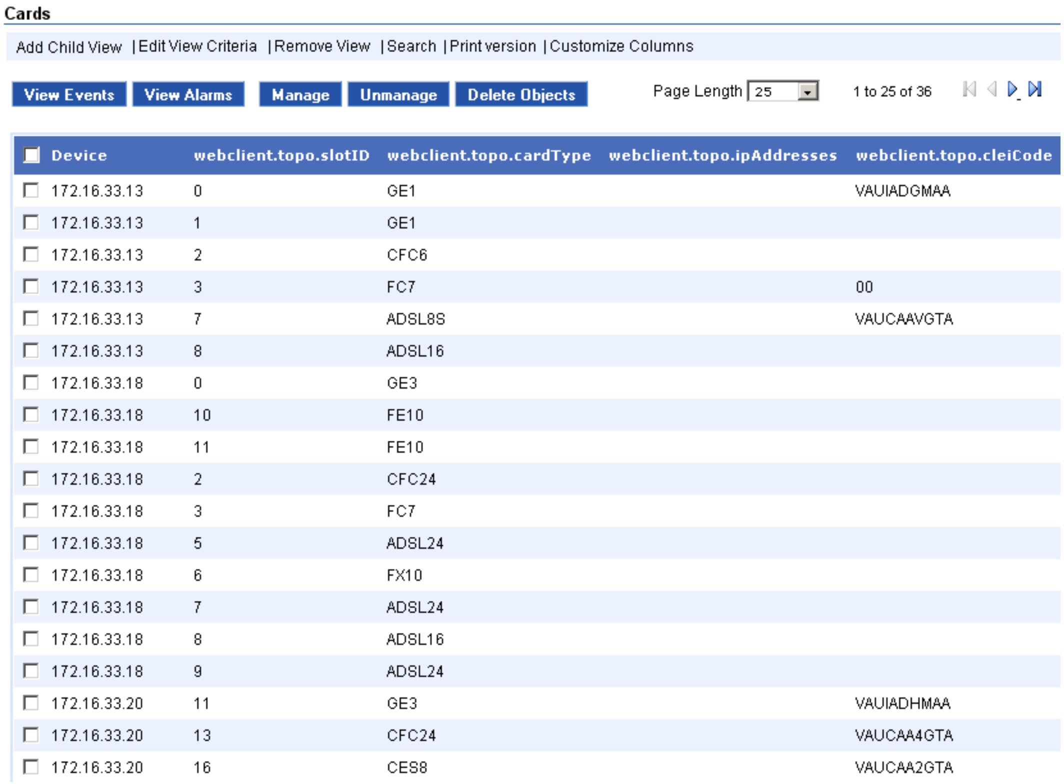
Page Length 25 — 1 to 18 of 18

□ Name	Type	IP Address	Profile
□ 172.16.33.1	Rapier48	172.16.33.1	
□ 172.16.33.10	RapierG6fsx	172.16.33.10	
□ 172.16.33.11	7700	172.16.33.11	
□ 172.16.33.12	AT-AR725	172.16.33.12	
□ 172.16.33.13	7400	172.16.33.13	
□ 172.16.33.16	Rapier24i	172.16.33.16	
□ 172.16.33.18	9400	172.16.33.18	
□ 172.16.33.19	7103	172.16.33.19	
□ 172.16.33.2	AT-8748XL	172.16.33.2	
□ 172.16.33.20	9700	172.16.33.20	
□ 172.16.33.25	AT-AR250E	172.16.33.25	
□ 172.16.33.26	AT-AR745	172.16.33.26	
□ 172.16.33.27	AT-8948	172.16.33.27	
□ 172.16.33.29	AT-AR720	172.16.33.29	
□ 172.16.33.3	Rapier24	172.16.33.3	
□ 172.16.33.33	RG613-TX	172.16.33.33	
□ 172.16.33.4	SB4104AC	172.16.33.4	
□ 172.16.33.6	Rapier24	172.16.33.6	

FIGURE 33-18 Profile Association

TABLE 33-8 Profile View Columns

Column	Meaning
Name	The object name. The icon to the left of the name (such as ✥) is the icon for a network node object, which is the object type, where the icon color depicts current criticality state of the object. Left-clicking the name brings up the Object Details form. The arrow to the right of the name (») brings up a menu of appropriate actions (Manage/ Unmanage). Left-clicking the arrow brings up the menu.
Type	The device type (the type of AT device).
IPAddress	The object IP address.
Profile	The associated Profile

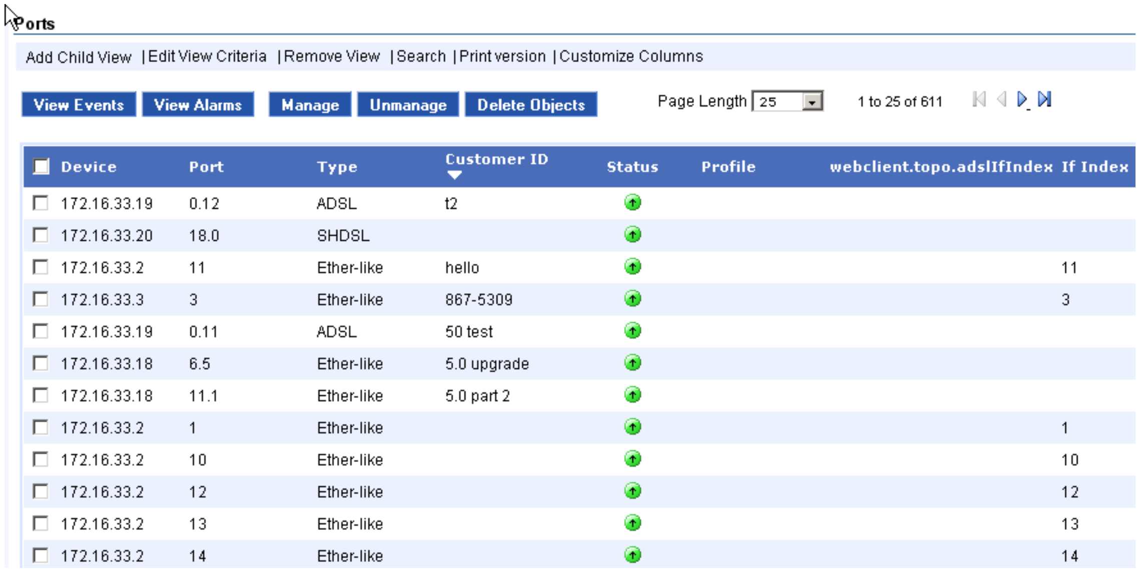

Cards
Add Child View | Edit View Criteria | Remove View | Search | Print version | Customize Columns
View Events
View Alarms
Manage
Unmanage
Delete Objects
Page Length 25
1 to 25 of 36

□ Device	webclient.topo.slotID	webclient.topo.cardType	webclient.topo.ipAddresses	webclient.topo.cleiCode
□ 172.16.33.13	0	GE1		VAUIADGMAA
□ 172.16.33.13	1	GE1		
□ 172.16.33.13	2	CFC6		
□ 172.16.33.13	3	FC7		00
□ 172.16.33.13	7	ADSL8S		VAUCAAVGTA
□ 172.16.33.13	8	ADSL16		
□ 172.16.33.18	0	GE3		
□ 172.16.33.18	10	FE10		
□ 172.16.33.18	11	FE10		
□ 172.16.33.18	2	CFC24		
□ 172.16.33.18	3	FC7		
□ 172.16.33.18	5	ADSL24		
□ 172.16.33.18	6	FX10		
□ 172.16.33.18	7	ADSL24		
□ 172.16.33.18	8	ADSL16		
□ 172.16.33.18	9	ADSL24		
□ 172.16.33.20	11	GE3		VAUIADHMAA
□ 172.16.33.20	13	CFC24		VAUCAA4GTA
□ 172.16.33.20	16	CES8		VAUCAA2GTA

FIGURE 33-19 Card Inventory View

TABLE 33-9 Cards View Columns

Column	Meaning
Device	The device that contains the card
Slot	The slot number of the card
Type	The type of card.
IP Address	For cards that require an IP interface (POTS24, CES8)
CLEI Code	For cards that have a CLEI code



Ports

Add Child View | Edit View Criteria | Remove View | Search | Print version | Customize Columns

Page Length 25

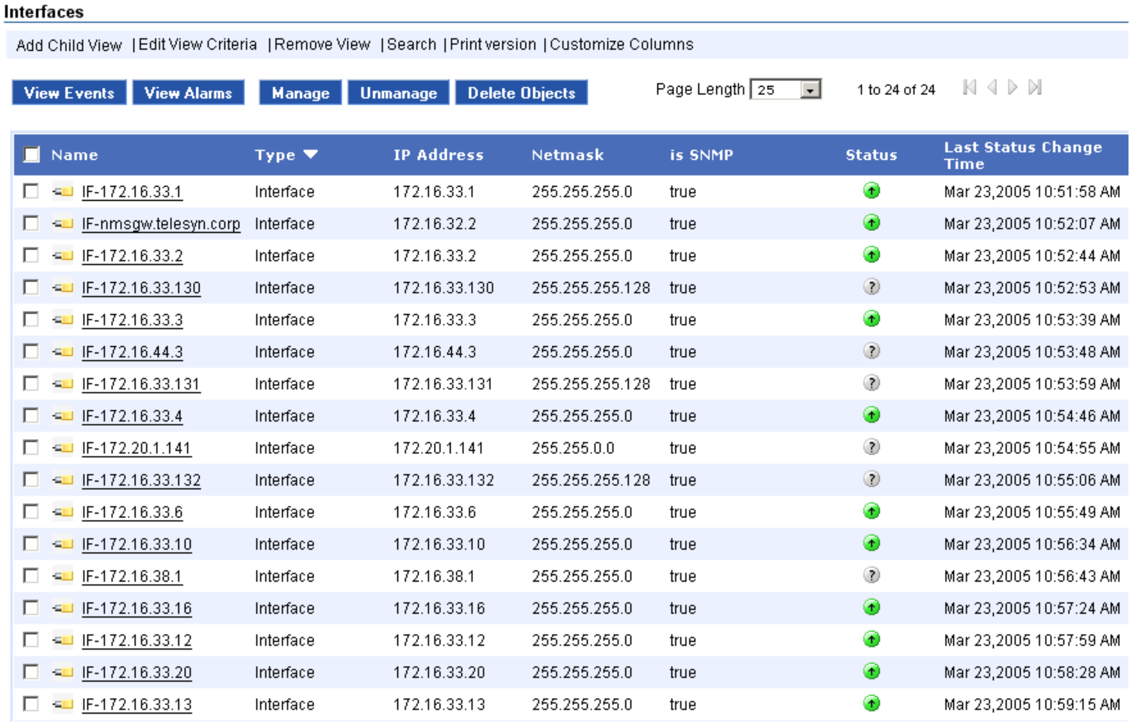
1 to 25 of 611

□ Device	Port	Type	Customer ID	Status	Profile	webclient.topo.adslIfIndex	If Index
□ 172.16.33.19	0.12	ADSL	t2	●			
□ 172.16.33.20	18.0	SHDSL		●			
□ 172.16.33.2	11	Ether-like	hello	●			11
□ 172.16.33.3	3	Ether-like	867-5309	●			3
□ 172.16.33.19	0.11	ADSL	50 test	●			
□ 172.16.33.18	6.5	Ether-like	5.0 upgrade	●			
□ 172.16.33.18	11.1	Ether-like	5.0 part 2	●			
□ 172.16.33.2	1	Ether-like		●			1
□ 172.16.33.2	10	Ether-like		●			10
□ 172.16.33.2	12	Ether-like		●			12
□ 172.16.33.2	13	Ether-like		●			13
□ 172.16.33.2	14	Ether-like		●			14

FIGURE 33-20 Customer Ports View

TABLE 33-10 Customer Ports View Columns

Column	Meaning
Device	The node name
Port	The port number on the card. Typically, the port number is the customer’s telephone number
Type	The interface for the port
Customer ID	An ID number that uniquely identifies the port.
Status	The current status of the port.
Profile	The profile the port has been associated with. If there is an *, the data on the port and the associated profile do not match.
ADSL IfIndex	Index number created for the ADSL port
ifIndex	Index number created for the ethernet port



Interfaces

Add Child View | Edit View Criteria | Remove View | Search | Print version | Customize Columns

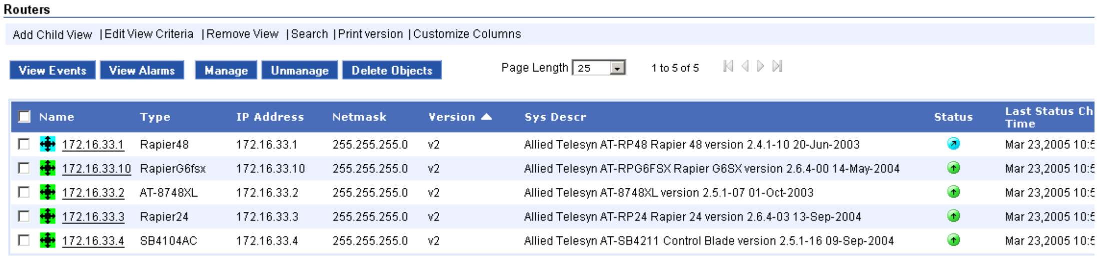
View Events | View Alarms | Manage | Unmanage | Delete Objects   Page Length 25   1 to 24 of 24

□	Name	Type ▼	IP Address	Netmask	is SNMP	Status	Last Status Change Time
□	IF-172.16.33.1	Interface	172.16.33.1	255.255.255.0	true	↑	Mar 23,2005 10:51:58 AM
□	IF-nmsgw.telesyn.corp	Interface	172.16.32.2	255.255.255.0	true	↑	Mar 23,2005 10:52:07 AM
□	IF-172.16.33.2	Interface	172.16.33.2	255.255.255.0	true	↑	Mar 23,2005 10:52:44 AM
□	IF-172.16.33.130	Interface	172.16.33.130	255.255.255.128	true	?	Mar 23,2005 10:52:53 AM
□	IF-172.16.33.3	Interface	172.16.33.3	255.255.255.0	true	↑	Mar 23,2005 10:53:39 AM
□	IF-172.16.44.3	Interface	172.16.44.3	255.255.255.0	true	?	Mar 23,2005 10:53:48 AM
□	IF-172.16.33.131	Interface	172.16.33.131	255.255.255.128	true	?	Mar 23,2005 10:53:59 AM
□	IF-172.16.33.4	Interface	172.16.33.4	255.255.255.0	true	↑	Mar 23,2005 10:54:46 AM
□	IF-172.20.1.141	Interface	172.20.1.141	255.255.0.0	true	?	Mar 23,2005 10:54:55 AM
□	IF-172.16.33.132	Interface	172.16.33.132	255.255.255.128	true	?	Mar 23,2005 10:55:06 AM
□	IF-172.16.33.6	Interface	172.16.33.6	255.255.255.0	true	↑	Mar 23,2005 10:55:49 AM
□	IF-172.16.33.10	Interface	172.16.33.10	255.255.255.0	true	↑	Mar 23,2005 10:56:34 AM
□	IF-172.16.38.1	Interface	172.16.38.1	255.255.255.0	true	?	Mar 23,2005 10:56:43 AM
□	IF-172.16.33.16	Interface	172.16.33.16	255.255.255.0	true	↑	Mar 23,2005 10:57:24 AM
□	IF-172.16.33.12	Interface	172.16.33.12	255.255.255.0	true	↑	Mar 23,2005 10:57:59 AM
□	IF-172.16.33.20	Interface	172.16.33.20	255.255.255.0	true	↑	Mar 23,2005 10:58:28 AM
□	IF-172.16.33.13	Interface	172.16.33.13	255.255.255.0	true	↑	Mar 23,2005 10:59:15 AM

FIGURE 33-21 Interface Inventory View (HTML)

TABLE 33-11 Interface View Columns

Column	Meaning
Name	The object name. The icon to the left of the name ( ) is the icon for an interface object, which is the object type, where the icon color depicts current criticality state of the object. Left-clicking the name brings up the Object Details form.
Type	The object type (interface).
IPAddress	The object IP address.
NetMask	The object subnetwork or network category.
IsSNMP	The state of SNMP in the device (enabled or disabled).
Status	The alert status.
Last Status Time Change	The date and time at which the object information was last updated.

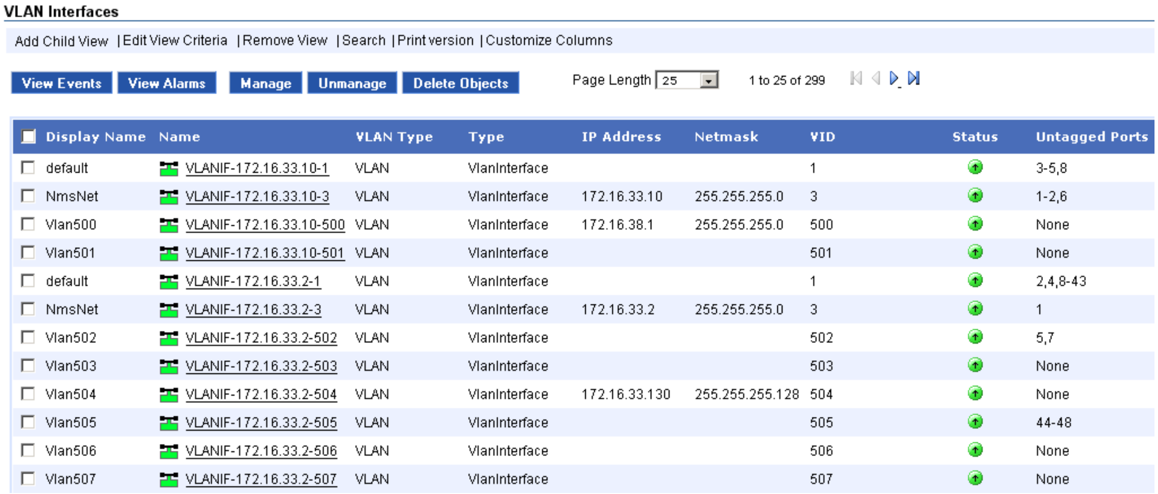

Routers
Add Child View | Edit View Criteria | Remove View | Search | Print version | Customize Columns
View Events
View Alarms
Manage
Unmanage
Delete Objects
Page Length 25
1 to 5 of 5

☐	Name	Type	IP Address	Netmask	Version ▲	Sys Descr	Status	Last Status Ch Time
☐	172.16.33.1	Rapier48	172.16.33.1	255.255.255.0	v2	Allied Telesyn AT-RP48 Rapier 48 version 2.4.1-10 20-Jun-2003	●	Mar 23,2005 10:5
☐	172.16.33.10	RapierG6fsx	172.16.33.10	255.255.255.0	v2	Allied Telesyn AT-RPG6FSX Rapier G6SX version 2.6.4-00 14-May-2004	●	Mar 23,2005 10:5
☐	172.16.33.2	AT-8748XL	172.16.33.2	255.255.255.0	v2	Allied Telesyn AT-8748XL version 2.5.1-07 01-Oct-2003	●	Mar 23,2005 10:5
☐	172.16.33.3	Rapier24	172.16.33.3	255.255.255.0	v2	Allied Telesyn AT-RP24 Rapier 24 version 2.6.4-03 13-Sep-2004	●	Mar 23,2005 10:5
☐	172.16.33.4	SB4104AC	172.16.33.4	255.255.255.0	v2	Allied Telesyn AT-SB4211 Control Blade version 2.5.1-16 09-Sep-2004	●	Mar 23,2005 10:5

FIGURE 33-22 Routers Inventory View (html)

TABLE 33-12 Routers View Columns

Column	Meaning
Name	The object name. The icon to the left of the name (✥) is the icon for a router object, which is the object type, where the icon color depicts current criticality state of the object. Left-clicking the name brings up the Object Details form. The arrow to the right of the name (») brings up a menu of appropriate actions (Manage/ Unmanage). Left-clicking the arrow brings up the menu.
Type	The object type (AT device).
IPAddress	The object IP address.
NetMask	The object subnetwork or network category.
Version	The version of SNMP (v1 or v2) in the object.
System Descr	The detailed name of the device and software load running.
Status	The alert status.
Last Status Time Change	The date and time at which the object information was last updated.

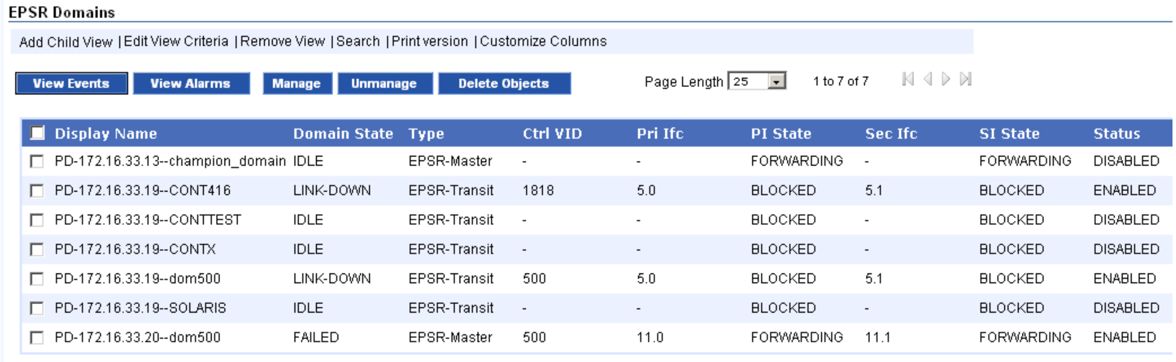

VLAN Interfaces
Add Child View | Edit View Criteria | Remove View | Search | Print version | Customize Columns
View Events
View Alarms
Manage
Unmanage
Delete Objects
Page Length 25
1 to 25 of 299

☐ Display Name	Name	VLAN Type	Type	IP Address	Netmask	VID	Status	Untagged Ports
☐ default	VLANIF-172.16.33.10-1	VLAN	VlanInterface			1	●	3-5,8
☐ NmsNet	VLANIF-172.16.33.10-3	VLAN	VlanInterface	172.16.33.10	255.255.255.0	3	●	1-2,6
☐ Vlan500	VLANIF-172.16.33.10-500	VLAN	VlanInterface	172.16.38.1	255.255.255.0	500	●	None
☐ Vlan501	VLANIF-172.16.33.10-501	VLAN	VlanInterface			501	●	None
☐ default	VLANIF-172.16.33.2-1	VLAN	VlanInterface			1	●	2,4,8-43
☐ NmsNet	VLANIF-172.16.33.2-3	VLAN	VlanInterface	172.16.33.2	255.255.255.0	3	●	1
☐ Vlan502	VLANIF-172.16.33.2-502	VLAN	VlanInterface			502	●	5,7
☐ Vlan503	VLANIF-172.16.33.2-503	VLAN	VlanInterface			503	●	None
☐ Vlan504	VLANIF-172.16.33.2-504	VLAN	VlanInterface	172.16.33.130	255.255.255.128	504	●	None
☐ Vlan505	VLANIF-172.16.33.2-505	VLAN	VlanInterface			505	●	44-48
☐ Vlan506	VLANIF-172.16.33.2-506	VLAN	VlanInterface			506	●	None
☐ Vlan507	VLANIF-172.16.33.2-507	VLAN	VlanInterface			507	●	None

FIGURE 33-23 VLAN Interfaces View (html)

TABLE 33-13 VLAN Interface View Columns

Column	Meaning
Display Name	Matches the name given for the associated VLAN
Name	The object name. The icon to the left of the name (🟩) is the icon for an interface object (VLAN interface, in this case), which is the object type, where the icon color depicts current criticality state of the object. Left-clicking the name brings up the Object Details form.
VLAN Type	Default is VLAN
ID	The object (interface) ID.
Type	The object type (AT device).
IPAddress	The object IP address.
NetMask	The object subnetwork or network category.
VID	The version of SNMP (v1 or v2).
Status	The object status.
UnTagged Ports	The ports on the VLAN interface object that are untagged.
Tagged Ports	The ports on the VLAN interface object that are tagged.
Device	The device on which the VLAN IF resides
Network Vlan	The name of the VLAN if crosses multiple devices.
Forwarding Mode	For the UFO VLAN interface, the type of Forwarding used. (Standard VLANs do not have Forwarding configured.)
Node Type	Whether the Node is a Primary Upstream Node (into the upstream network), Secondary Upstream Node, or Non-Upstream
Pri UP Node Status	The status of the Primary Upstream Node (should be active)
Sec UP Node Status	The status of the Secondary Upstream Node (if configured, should be standby)


EPSR Domains
Add Child View | Edit View Criteria | Remove View | Search | Print version | Customize Columns
View Events
View Alarms
Manage
Unmanage
Delete Objects

Page Length 25

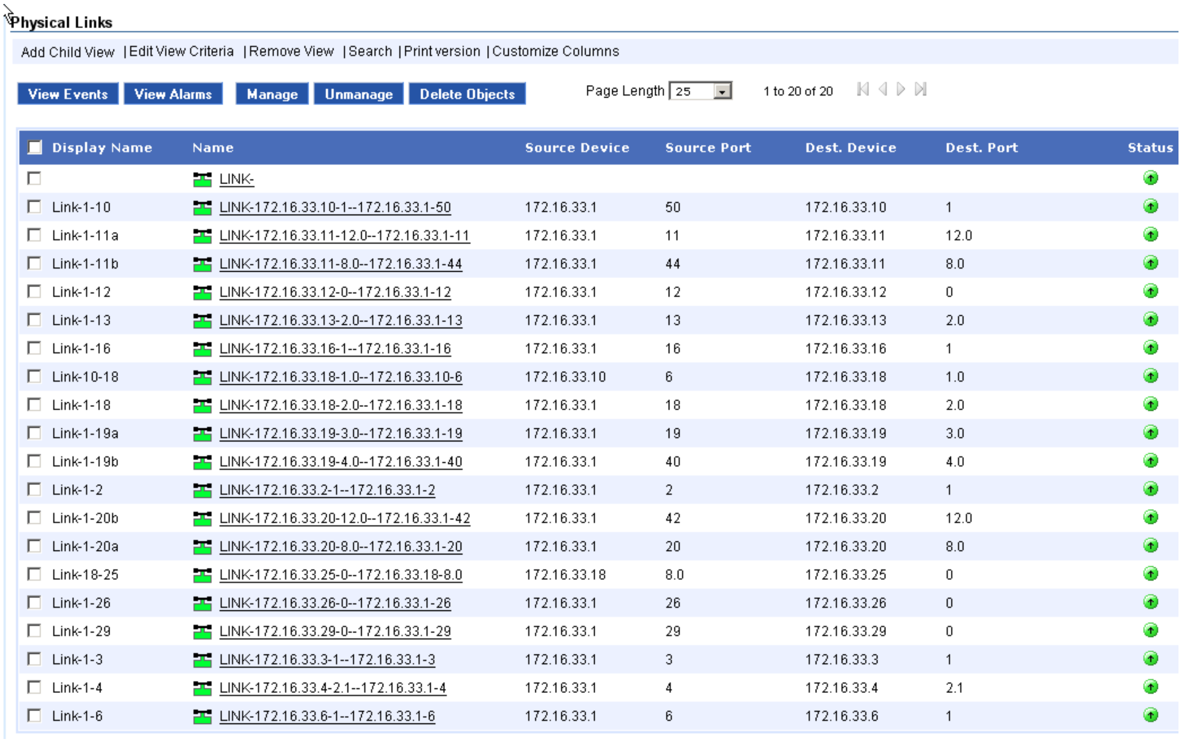
1 to 7 of 7

☐ Display Name	Domain State	Type	Ctrl VID	Pri Ifc	PI State	Sec Ifc	SI State	Status
☐ PD-172.16.33.13--champion_domain	IDLE	EPSR-Master	-	-	FORWARDING	-	FORWARDING	DISABLED
☐ PD-172.16.33.19--CONT416	LINK-DOWN	EPSR-Transit	1818	5.0	BLOCKED	5.1	BLOCKED	ENABLED
☐ PD-172.16.33.19--CONTTEST	IDLE	EPSR-Transit	-	-	BLOCKED	-	BLOCKED	DISABLED
☐ PD-172.16.33.19--CONTX	IDLE	EPSR-Transit	-	-	BLOCKED	-	BLOCKED	DISABLED
☐ PD-172.16.33.19--dom500	LINK-DOWN	EPSR-Transit	500	5.0	BLOCKED	5.1	BLOCKED	ENABLED
☐ PD-172.16.33.19--SOLARIS	IDLE	EPSR-Transit	-	-	BLOCKED	-	BLOCKED	DISABLED
☐ PD-172.16.33.20--dom500	FAILED	EPSR-Master	500	11.0	FORWARDING	11.1	FORWARDING	ENABLED

FIGURE 33-24 EPSR Domain View

TABLE 33-14 EPSR Domain View Columns

Column	Meaning
Display Name	Matches the name given for the associated VLAN
Name	The domain name that applies to this specific Network VLAN and all of its associated nodes.
Domain State	The overall state of the EPSR domain. LINK DOWN means one (or more) of the data VLANs has been broken.
Type	Whether the Domain is a Master or Transit
Ctrl VID	The VID of the network VLAN that is being used to create the protection ring
Pri Ifc	The interface for the associated VLAN with a state of Primary
PI State	The state of the Primary interface (BLOCKED or FORWARDING)
PI Prio	The priority number for the Primary Interface,
Sec Ifc	The interface for the associated VLAN with a state of Secondary
SI State	The state of the Secondary interface. (BLOCKED or FORWARDING
SI Prio	The priority number for the Secondary Interface,
Status	The overall state of the domain (whether it is ENABLED or DISABLED)



Physical Links

Add Child View | Edit View Criteria | Remove View | Search | Print version | Customize Columns

Page Length 25 1 to 20 of 20

□ Display Name	Name	Source Device	Source Port	Dest. Device	Dest. Port	Status
□	LINK-					●
□ Link-1-10	LINK-172.16.33.10-1--172.16.33.1-50	172.16.33.1	50	172.16.33.10	1	●
□ Link-1-11a	LINK-172.16.33.11-12.0--172.16.33.1-11	172.16.33.1	11	172.16.33.11	12.0	●
□ Link-1-11b	LINK-172.16.33.11-8.0--172.16.33.1-44	172.16.33.1	44	172.16.33.11	8.0	●
□ Link-1-12	LINK-172.16.33.12-0--172.16.33.1-12	172.16.33.1	12	172.16.33.12	0	●
□ Link-1-13	LINK-172.16.33.13-2.0--172.16.33.1-13	172.16.33.1	13	172.16.33.13	2.0	●
□ Link-1-16	LINK-172.16.33.16-1--172.16.33.1-16	172.16.33.1	16	172.16.33.16	1	●
□ Link-10-18	LINK-172.16.33.18-1.0--172.16.33.10-6	172.16.33.10	6	172.16.33.18	1.0	●
□ Link-1-18	LINK-172.16.33.18-2.0--172.16.33.1-18	172.16.33.1	18	172.16.33.18	2.0	●
□ Link-1-19a	LINK-172.16.33.19-3.0--172.16.33.1-19	172.16.33.1	19	172.16.33.19	3.0	●
□ Link-1-19b	LINK-172.16.33.19-4.0--172.16.33.1-40	172.16.33.1	40	172.16.33.19	4.0	●
□ Link-1-2	LINK-172.16.33.2-1--172.16.33.1-2	172.16.33.1	2	172.16.33.2	1	●
□ Link-1-20b	LINK-172.16.33.20-12.0--172.16.33.1-42	172.16.33.1	42	172.16.33.20	12.0	●
□ Link-1-20a	LINK-172.16.33.20-8.0--172.16.33.1-20	172.16.33.1	20	172.16.33.20	8.0	●
□ Link-18-25	LINK-172.16.33.25-0--172.16.33.18-8.0	172.16.33.18	8.0	172.16.33.25	0	●
□ Link-1-26	LINK-172.16.33.26-0--172.16.33.1-26	172.16.33.1	26	172.16.33.26	0	●
□ Link-1-29	LINK-172.16.33.29-0--172.16.33.1-29	172.16.33.1	29	172.16.33.29	0	●
□ Link-1-3	LINK-172.16.33.3-1--172.16.33.1-3	172.16.33.1	3	172.16.33.3	1	●
□ Link-1-4	LINK-172.16.33.4-2.1--172.16.33.1-4	172.16.33.1	4	172.16.33.4	2.1	●
□ Link-1-6	LINK-172.16.33.6-1--172.16.33.1-6	172.16.33.1	6	172.16.33.6	1	●

FIGURE 33-25 Physical Links View

TABLE 33-15 Physical Links View Columns

Column	Meaning
Display Name	Matches the name given to the link.
Name	The name supplied when the link was created (optional) The icon to the left of the name (such as 🟩) is the icon for a link object, which is the object type, where the icon color depicts current criticality state of the object. Left-clicking the name brings up the Object Details form
Source Device	The source node name
Source Port	The port on the source device to which the link is attached
Dest. Device	The destination node name
Dest. Port	The destination port
Status	The alert status
Link Type	The link type, especially if used for a feature, such as LAG
Discovery	The protocol used for discovery, usually LLDP

33.6.1 Network Inventory View Options

The options from Network Views (Add Child View, Edit View Criteria, etc.) are similar to other views. Refer to Alarm View Options for details. Also the options for individual objects, once selected using the tic box, are similar to other views.

The necessary details of network objects are available in a form called the Properties form. The properties of an object are displayed by clicking on the underlined value for a column, usually Name..

TABLE 33-16 Properties Form for Network Objects

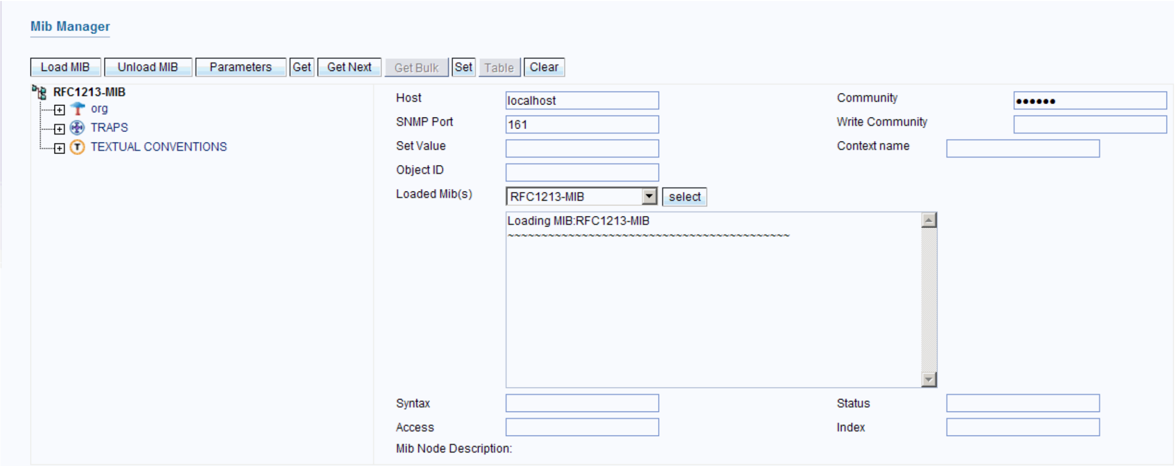
Type	Area	Detail
General (All objects)	General Information	Device Type Status Is Managed Display Name
	Identification Details	IP Address Netmask Is DHCP Enabled?
Monitoring (All objects)	Status Monitoring Details	Is Status Polling Enabled Tester for Status Polling Last Status Update Time Last Status Change Time User Class Name Failure Threshold Failure Count Status Polling Interval
Discovery (Network objects only)		Discovery Status Start / Resume Discovery
Network Elements (Network objects only)	Nodes & Interface Details	List of Nodes List of Interfaces Sub Networks Sub Netmask Parent Netmask Parent Network
Relationship (All objects except networks)	Interfaces & Parent Networks	List of Interfaces Parent Networks
	Logical & Hierarchical Relationship Details	Parent Object List of Groups Children keys View Details

TABLE 33-16 Properties Form for Network Objects

Type	Area	Detail
Protocol Setting (All objects except networks and links)	Protocol Configuration Settings	SNMP Port - Base MIBs Read Community Write Community SNMP Version
	Interface	Physical Media Physical Address Interface Speed Interface Description
SNMP (All objects except networks, links, and VLANs)	SNMP Details	System Object Identifier (SysOID) System Description Host Netmask

33.7 Working with SNMP Tools (MIB Manager)

The MIB Browser is displayed by selecting the *SNMP Tools* tab from the HTML menu, as shown in the following figure.



Host: localhost
SNMP Port: 161
Set Value:
Object ID:
Loaded Mib(s): RFC1213-MIB
Community: ••••••
Write Community:
Context name:

```
Loading MIB:RFC1213-MIB
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Syntax:
Access:
Mib Node Description:
Status:
Index:

FIGURE 33-26 MIB Browser (HTML)

The functionality of HTML UI MIB Browser is similar to that of the Java UI MIB Browser. The difference is that MIB Browser of the Java UI has some more advanced features in addition to the features found in HTML UI.

The HTML UI MIB Browser allows "**GET**", "**GETNEXT**", "**GETBULK**", and "**SET**" SNMP requests to a particular variable in the MIB of an SNMP managed device. It also allows table viewing. Apart from these features, the UI of the HTML UI MIB Browse represents and differentiates the various objects under the MIB with unique icons. In addition, the selected node under the MIB is highlighted with specific colors for easy identification as shown in Figure 33-26.

The left-side frame is the MIB tree, in which the selected MIB file is shown, and the right-side frame is for setting the options and for the result display. The right frame includes fields for:

- the current Node Object ID that's being operated upon the current MIB module
- the SNMP agent name or address (Host)

- the community name
- a text field to enter the value for the set operation
- a Write Community value, which is used for a set request
- a drop-down box that shows the currently loaded MIBs
- a text area to view query results

TRAP definitions and textual conventions for a specific MIB can be viewed by choosing the TRAPS node or the TEXTUAL CONVENTIONS node from the tree-view of MIB Browser.

The operations allowed with the HTML UI MIB Browser are available through the various icons in the toolbar at the top of the frame, which are shown in the following table.

TABLE 33-17 Task List for HTML Interface

Action	Meaning
Load MIB	Load the MIB files in the HTML UI MIB Browser.
UnLoad MIB	Unload the MIB files in the HTML UI MIB Browser.
Parameters	Sets the values for port, version, time-out, retries and max-repetitions. This displays a dialog where the Snmp Version, Snmp Port, Time-out, Retries, Max-Repetitions can be specified
Get	Performs a GET operation. This gets all the objects under the selected MIB object, or the specific object if the MIB node and instance are specified
GetNext	Performs a GETNEXT operation. This gets the next object after the specified object, or the specific object instance if a MIB node is specified.
GetBulk	Performs a GETBULK operation. This gets a sequence of Next Objects immediately after the specified object. The number returned Object instances are equal to the Max-Repetitions field.
Set	performs a SET operation. This enables setting the value of the specified object, based on the value in the **Set Value** field. To do a SET for Octet String Type in hex format enter the bytes in hex format with each bytes separated by a colon and the entire string within single quotes. For example to give 0xff0a3212 enter 'ff:0a:32:12' in the SetValue field
Table	Allows you to view the SNMP Table. This brings the display of SnmpTable, if the selected OID is a table
Clear	Clears the text area. It clears the QUERY RESULTS, which sometimes overflow its capacity and needs to be cleared

The **select** button, in the right-side frame, is used to select the MIB to be displayed in the tree-view of HTML Client.
Apart from these, there are text fields for displaying Syntax, Access, Status, Index, and MIB Node Description, which give a brief description of the selected MIB file

Note: The UI of HTML UI MIB Browser is not the same as that of Java UI MIB Browser. Apart from the difference in the UI, some of the features present in the Java UI MIB Browser such as v3 support, graphing, etc., are not available in the HTML UI MIB Browser

33.7.1 Loading and Unloading MIBs

The MIB files can be loaded or unloaded as per your requirements. To load the MIB files, use the **Load MIB** option. This displays the HTML page with the list of MIBs.

The MIB Browser allows loading of compiled MIB files. To store the compiled information, there are two file types are used for storing the MIB information in a formatted structure:

- cmi - This file type contains MIB information such as MIB node, MIB module, naming hierarchy, etc.
- cds - This file type contains the description and reference of the nodes in the MIB.

The compiled MIB files reduce the loading time leading to performance improvement. The **Load MIBs from compiled Files** check box can be checked/unchecked to load the MIB files directly or as compiled MIB files. By default, this option is unchecked. If this is unchecked, you can directly load the MIB file, as provided.

When **Load MIBs from compiled File** is enabled, the MIB Browser tries to load the **.cmi** and **.cds** file, if they are present. Otherwise, this parses the MIB file and writes the output in **.cmi** and **.cds** files and then loads the MIB file. For example, for RFC1213-MIB, the compiled MIB files are **RFC1213-MIB.cmi** and **RFC1213-MIB.cds**. The advantage of using this option is that we need not parse the MIB each time we load it, thus optimizing the loading time.

While loading the compiled MIBs it is enough if we load the **.cmi** file alone. The **.cmi** file has reference to the**.cds** files. The <mib_file_name>**.cds** file should not be loaded directly.

After loading the MIB file as a compiled MIB file, any change done in the MIB file doesn't get reflected in the loaded MIB file. You have to remove the existing **.cmi** and **.cds** files, and then load the MIB to get the latest changes done. The **Overwrite existing compiled MIB files** check box can be enabled to overcome this. If this option is set to True, the **.cmi** and **.cds** files are created each time the MIB is loaded.

Enabling this option is recommended only if you have changed the contents of the MIB file. Otherwise, this unnecessarily increases the load time of the MIBs.

The MIB files displayed in the list box (as shown in the above screen) are provided in the *<NMS Home>/mibs* directory. It may be convenient to copy your MIB files to be loaded, into the *<NMS Home>/mibs* directory.

Choose the MIB to be loaded from the list box displayed and choose the **Load** button.

You can also load multiple MIBs, which get displayed in the list box provided, as shown in Figure 33-26. Select one of the listed MIBs from the list box. Use the **Load** button to display it in the tree-view of HTML Client. When any MIB module is selected, the root node for that MIB becomes the current OID.

Note: *The tree-view of HTML UI MIB Browser displays only one MIB at any time. To view the objects of another MIB file, you need to select the respective MIB file from the list box which gets overwritten in the tree-view.*

To unload the loaded MIB, select the node from the MIB Tree and then choose the **Unload** option from the MIB Toolbar. This removes the MIB and its reference from the tree.

33.7.2 MIB Browser Settings

The third icon in the toolbar at the top of the frame is the **Parameters** icon. This option allows configuration of various options needed for SNMP operations.

You can modify the default values as per your requirements. The following table shows the options, description, its default values, and other options available.

TABLE 33-18 MIB Browser Settings

Options fir MIB Browser	Description	Default Values	Other Options
Snmp Version	The version of the SNMP used.	SNMP_ Version1	SNMP_Version2c
Snmp Port	The port where the SNMP agent listens.	161	any user-defined port
Time out (Sec)	The duration for the SNMP request to wait for the response from any device.	5	any user-defined value

TABLE 33-18 (Continued)MIB Browser Settings

Retries	The number of times the SNMP manager should make the request to the SNMP agent.	0	any user-defined value
Max. repetitions (For GetBulk)	The number of Object instances to be returned for a given single request. (Applicable only to SNMP_Version2c)	50	any user-defined value
Non Repeaters	The number of pairs in the VarBindList array for which a single instance should be returned (only for SNMPv2c)		any user-defined value

33.7.3 SNMP Operations

The MIB Browser allows you to do typical SNMP operations, such as GET, GET NEXT, GET BULK, and SET. To do the GET operation, you have to load the MIB file, select the desired node, and click the **Get** button in the MIB toolbar, provided at the top of the frame. To fully specify an object to an SNMP agent, both the Object ID (which defines the type of object) and the instance (the specific object of the given type) need to be provided. From the MIB, you can get the Object ID, to which an instance needs to be added to completely identify the object of interest.

For non-tabular objects or scalar objects, this is simply an instance of 0 (e.g., sysDescr.0, this need not be specified the MIB Browser adds it to the selected node). For tabular objects, the instance is defined by the MIB and is a sequence of one or more variables (for example, ifInOctets.2 or tcpConnState.179.74.15.126.1192.225.226.126.197.80).

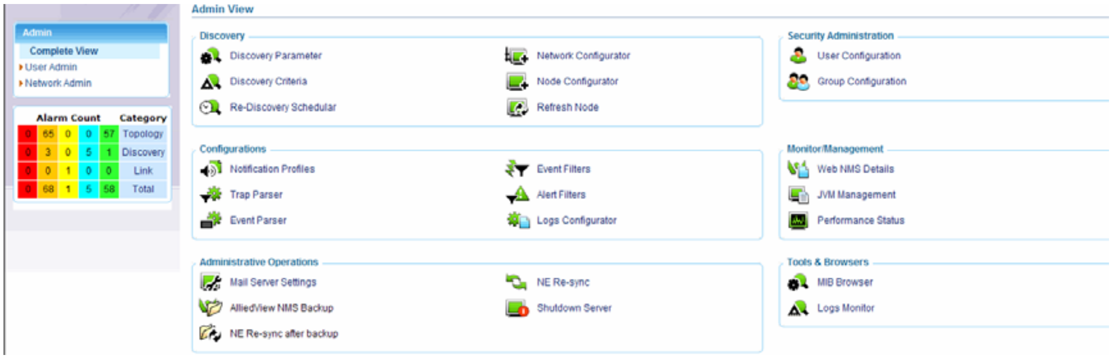
33.7.4 SNMP Table

To view the SNMP table, click the **Table** button in the MIB Toolbar provided at the top of the frame. This displays the SNMP Table if the selected OID is a table.

33.8 Admin (User and Network)

The Admin tab brings up the Administration screen. The options and what they mean are included in the screens.

Refer to the following figure.



Alarm Count					Category
0	65	0	0	57	Topology
0	3	0	5	1	Discovery
0	0	1	0	0	Link
0	68	1	5	58	Total

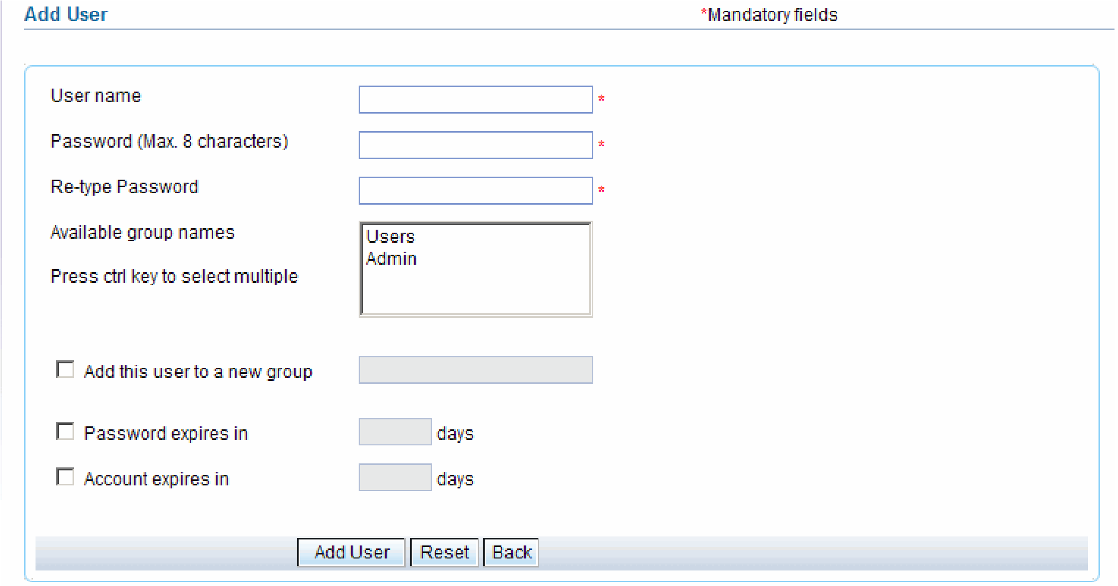
FIGURE 33-27 Admin Screen (html)

33.8.1 Security Administration

From the Security admin screen, the user chooses User Configuration, and can then add a user, modify the user profile, or remove a user.

33.8.1.1 User Configuration

The Add User form is shown in the following figure. Table 33-19 lists the options.



Add User *Mandatory fields

User name *

Password (Max. 8 characters) *

Re-type Password *

Available group names

Press ctrl key to select multiple

Users
Admin

□ Add this user to a new group

□ Password expires in days

□ Account expires in days

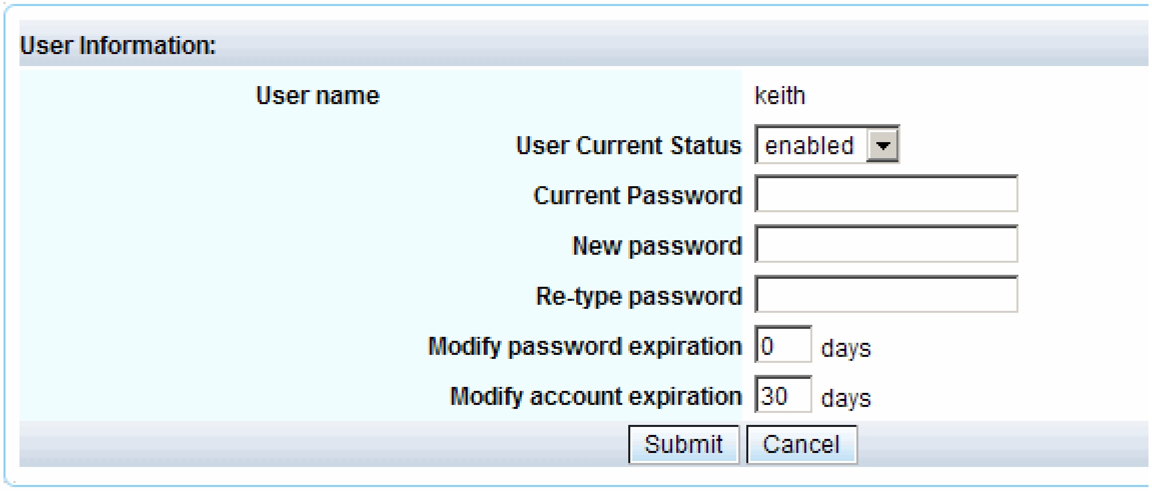
FIGURE 33-28 Add User Screen (html)

TABLE 33-19 Options for Add User

Field	Meaning
User Name	Required, the name must be unique with up to NEED INFO characters.
Password	Required, the password must be unique with up to NEED INFO characters. The Re-type Password must match or there is an error message.
Available group names	The option to add the user to a group, so that the user inherits the privileges of the group.
Add this user to a new group	Checking the tic box activates the field, and a new group can be defined that includes the new user. NEED INFO - what privileges does the new user have? always admin?
Password expires in	Checking the tic box activates the field, how many days the password is valid.
Account expires in	Checking the tic box activates the field, how many days the user name is valid.

33.8.1.2 Modify User Profile

To modify the User Profile, select the Edit icon. The Modify User Profile form is shown in the following figure. Table 33-20 lists the fields.



User Information:

User name	keith
User Current Status	enabled
Current Password	
New password	
Re-type password	
Modify password expiration	0 days
Modify account expiration	30 days

FIGURE 33-29 Modify User Profile Screen (html)

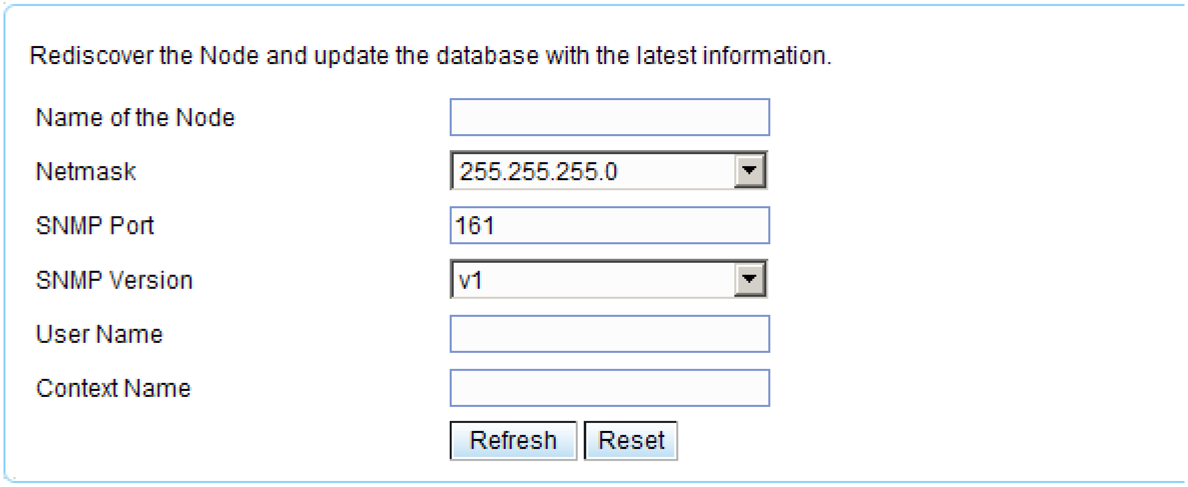
TABLE 33-20 Options for Modify User Profile

Field	Meaning
Current and New Password	Checking the tic box activates the field, and a new password can be defined.
Groups	Which groups the user can belong in. The user must belong in at least one group. More than one group can be chosen using the right and left arrows.
Modify password expiration	Checking the tic box activates the field, how many days the password is valid.
Modify password expiration	Checking the tic box activates the field, how many days the user name is valid.

33.8.2 Network Admin

The options here allow the user to add a node, add a network, and refresh a node.

The refresh node form is shown in the following figure.



Rediscover the Node and update the database with the latest information.

Name of the Node	
Netmask	255.255.255.0
SNMP Port	161
SNMP Version	v1
User Name	
Context Name	

FIGURE 33-30 Refresh a Node (html)

The name of the node is one of the node’s managed object properties. The Netmask is one of the pull-down options, and the SNMP port has the 161 default.

The refresh button, when selected, starts the rediscovery process **immediately** and updates the system with the most current node information.

33.8.3 Other Administrative Tasks

The following tables take each of the administrative areas shown in the other panels of the Admin Complete View and explain what they provide and when they would be used.

Note: Some of these tasks (such as Shutdown Server) are destructive and should only be done by authorized personnel.

TABLE 33-21 Admin Operations

Task	Description	Notes
Shutdown Server	Shuts down the server the client is connected with (FE or FE/BE).	**Perform this only if you are authorized to do so.**
NE Resync	Discards all the traps that are being processed by the server. Deletes the events and alerts from the database. Clears all the managed objects and updates the status by doing status poll.	

TABLE 33-22 Admin Configurations

Task	Description	Notes
Discovery Parameter	Controls Discovery Configuration Settings	Details on the fields in this from are in Security Administration. Perform this only if you are authorized to do so.
Discovery Criteria	Specifies the Managed Object properties based on which discovery can be enabled / disabled	Perform this only if you are authorized to do so.
Trap Parser	Creates and refines the information received from a trap (a specific unsolicited report by a device). The trap configuration can be imported using information the MIB or a file where the configuration is defined.	Details on the fields in this from are in Setting Up Fault Management. Trap parsers are critical to alarm correlation and should only be changed under the supervision of Allied Telesis Technical Support personnel.
Re-Discovery Scheduler	Set the schedule for re-discovery	Can be at regular interval (recurring) or on user-created schedule.
Notification Profiles		
Trap Parser	Controls Trap Parser Configuration list	
Event Parser	Controls Event Parser Configuration list	

TABLE 33-22 (Continued)Admin Configurations

Event Filters	Controls Event filters	These are loaded from and saved to conf/ event.filters
Alert FIlters	Controls Alert Filter Configuration list	These are loaded from and saved to conf/ alert.filters

TABLE 33-23 Server Details

Task	Description	Notes
Backend Details	Provides basic configuration information for BE server	This information is useful if reporting a AlliedView NMS error to Allied Telesis personnel.
Scheduler Details	Status of the main software tasks	
Frontend Details	Provides basic configuration information for FE server	Includes server mode as PRIMARY or SECONDARY, useful when in a distributed server configuration.
Client Details	Provides basic configuration information for client currently being used.	
Server Logs	Provides a list of NMS server logs; the user can click on each one and see the logging data	This information is useful if reporting a AlliedView NMS error to Allied Telesis personnel.
Logging	Controls how NMS logs will be written to log files	**Perform this only if you are authorized to do so.**

TABLE 33-24 Module Details

Task	Description	Notes
Discovery Status	Provides overall status of Discovery history for modules and networks	
Fault Status	Provides the status of the Fault Management system (events, alerts and traps processing), not faults on the devices	If not set at 0, server is still processing faults and so may not have the latest fault snapshot
Performance Status	Provides the performance status of a Node, using the node name to access User is also prompted for time period.	